Departamento de Informática

PROYECTO FIN DE CARRERA
I.T INFORMÁTICA DE GESTIÓN

GOBERNANZA CORPORATIVA DE LA TECNOLOGÍA DE LA INFORMACIÓN (T.I)
(Auditoría y Control según la norma UNE-ISO/IEC 38500:2013)

Autor: Elena Gómez González

Tutor: Miguel Ángel Ramos González

Leganés, Octubre de 2015

Título: Gobernanza corporativa de la Tecnología de la Información (T.I) (Auditoría y control según la norma UNE-ISO/IEC 38500:2013)
Autor: Elena Gómez González
Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día ____ de _____ de _____en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

En primer lugar, agradecer a Miguel Ángel su dedicación como tutor, consejos y palabras de ánimo.

A mi familia: Claudio, Elena, Lourdes y Rafa; y a la que considero casi como tal: Juan, Isabel y Daniel. Especialmente a T. Santiago, que seguro que estaría casi tan feliz como yo en este día.

A los compañeros de la uc3m con los que, a pesar de los años, sé que puedo seguir contando: Alberto, David, Jaime, Paco y Rodrigo.

A todas las personas que he conocido en este camino y a los que tengo el privilegio de contar como amigos: Esther, Laura, Ruth; Paco H., Raúl, Mónica, Ángel, Bernardino, J. Miguel, Óscar y Rui.

Y por supuesto a Juanra, ¡gracias por todo y por ser así!

No podía terminar sin hacer mención a la siguiente frase célebre, que seguro que todos los compañeros entenderán: “lo que no han separado las prácticas, no lo separa el hombre”.

Resumen

El gobierno corporativo define el contexto actual en el que las empresas deben evaluar y fijar, sus inversiones y los riesgos relacionados con el activo empresarial de la información y la infraestructura tecnológica, bajo la cual se recopila, manipula, almacena y se da uso a la información. ¿Pero qué es gobierno corporativo y por qué es importante para los profesionales T.I? ¿Y por qué el gobierno de las Tecnologías de la Información (T.I) debe ser conocido por los directivos de las empresas?

Este proyecto tiene como objetivo profundizar en dos aspectos principales.

El primero es comentar el papel estratégico de la tecnología de la información en la empresa y mencionar los riesgos asociados.

El segundo es dar a conocer los requisitos de gobierno corporativo y gobierno T.I y orientar acerca de los marcos y estándares relacionados. Cada una de estas normas y marcos tiene un carácter decisivo y de generación de valor en las organizaciones; el desafío es integrarlos de manera que cada uno cumpla el fin para el que fueron diseñados y que permitan a la entidad diseñar su propio gobierno T.I, en base a sus requerimientos y necesidades. Teniendo en cuenta estos aspectos, y como solución, se elabora una guía de implantación de gobierno T.I y un modelo de autoevaluación, diseñado para mejorar el gobierno de las operaciones T.I y hacerlas más eficientes. Este modelo soporta la implementación de la norma UNE-ISO/IEC 38500, el estándar internacional relacionado con las mejores prácticas de gobierno T.I, y está integrado con otro marco de referencia, COBIT 5.

Palabras clave: gobierno corporativo, gobierno T.I, Tecnologías de la Información, UNE-ISO/IEC 38500, COBIT 5.

Abstract

Corporate governance defines the current situation within which companies have to evaluate and establish, the investment and risks about company information assets and information technology infrastructure, which allows for collecting, manipulating, storing and giving use to information. Then, how can we define corporate governance and the reason why it's important to IT professionals? And why Information Technology governance should be known by organizations managers?

This project's going to delve into two main questions.

The first question it's about the Information Technology strategic role within a company and point out its associated risks.

The second one tries to get to know corporate governance and IT governance requirements and provide guidance on frameworks and related standards. Each of these frameworks and standards has a decisive role and adds value in organizations; the main difficulty is how integrate them so everyone keeps the purpose for which they were designed and allow the organization to design its IT government, based on their own requirements and needs. Considering these aspects, as solution, we elaborate a guide to implementing IT governance and a self-assessment model, designed to improve the governance of IT operations and increase their efficiency. This model implements the standard UNE-ISO/IEC 38500, the international standard related to IT governance best practices, and it's integrated with another main framework, COBIT 5.

Keywords: corporate governance, IT governance, Information Technology, UNE-ISO/IEC 38500, COBIT 5.

Índice general

Universidad Carlos III de Madrid

Índice de figuras

Índice de tablas

Capítulo 1
Introducción y objetivos

Se describe el objetivo general del propósito del proyecto, así como las fases de desarrollo, los medios empleados, los objetivos a alcanzar y la estructura de la memoria.

En el primer apartado del capítulo, *1.1 Introducción*, se presentan las motivaciones por las que se ha llevado a cabo este proyecto.

El segundo apartado, *1.2 Objetivos*, expone los objetivos a alcanzar.

En el apartado *1.3 Fases de desarrollo*, se detallan las fases necesarias para la realización del proyecto.

El cuarto apartado, *1.4 Medios empleados*, hace referencia a los medios con los que se ha contado.

Por último, en el punto *1.5 Estructura de la memoria*, se introducen los contenidos de cada uno de puntos principales que componen la memoria, aportando una visión general del proyecto.

1.1 Introducción

Basta con echar la vista atrás para percibir el desarrollo casi exponencial de las tecnologías encargadas de la gestión de la información: los libros de papel han sido casi reemplazados por eBooks; no hacen falta dispositivos físicos para almacenar la información, puede guardarse en la nube; desde nuestro móvil se pueden leer documentos, acceder a Internet… algo casi inimaginable hace dos décadas. Si este es el impacto a nivel de usuario pensemos en las organizaciones, en cómo tienen que incorporar en sus procesos diarios estos cambios, si quieren hacerlos más eficientes y en la optimización de costes y generación de beneficios que pueden generar, es decir, en la ventaja competitiva que son las tecnologías de la información (T.I).

Una mala gestión o la falta de controles T.I pueden provocar en la entidad una interrupción de los servicios, afectar a su imagen corporativa e incluso la quiebra. Las empresas y los auditores que las evalúan necesitan unas pautas definidas, unas normas que les ofrezcan garantía de conformidad en sus resultados. Esta necesidad de control, de cumplimiento, es extensible incluso a los servicios externos de las empresas, donde cada vez es más frecuente exigirles algún tipo de certificación relativa a la gestión de procesos, servicios y de la información.

La mayoría de los marcos y de normas que los complementan, relacionadas con las T.I, están orientadas hacia la gestión y no al gobierno, es decir, consideran la tecnología de la información como un servicio que puede ofrecerse a los clientes en lugar de enfocarse en cómo usarla.

En base a estas necesidades, en el año 2008 y partiendo de la norma australiana AS 8015, surge la UNE-ISO/IEC 38500 cuyo fin es garantizar la eficacia, eficiencia y aceptación del uso de la T.I en las organizaciones. La norma está compuesta por seis principios que proponen una serie de indicaciones a tener en cuenta en la toma de decisiones. A su vez, cada principio establece los objetivos a cumplir, pero no indica cómo llevarlos a cabo ni los responsables de su implantación.

Queda claro entonces, que los gestores que deseen un adecuado gobierno de las T.I para, entre otros, alcanzar los objetivos de negocio, identificar y controlar los riesgos T.I, optimizar sus procesos, etc., deben optar por el cumplimiento de la norma UNE-ISO/IEC 38500. Este va a ser el objetivo principal del proyecto, diseñar un modelo que permita evaluar el nivel de conformidad de cada uno de los principios y la implantación del gobierno T.I en una organización en base al estándar; en función de los resultados y los riesgos detectados en la evaluación, definir las actividades y planes necesarios para corregirlos, minimizar los riesgos y mejorar el nivel madurez de los principios. Tras la implementación de estas medidas se propone realizar una nueva evaluación con el fin de monitorizar el rendimiento de los cambios aplicados. El cumplimiento de esta funcionalidad hace que nuestro modelo propuesto se ajuste al ciclo Evaluar, Dirigir, Monitorizar planteado en la norma 38500, que es además es un ciclo de mejora continua.

1.2 Objetivos

Los objetivos principales que se pretenden alcanzar en este proyecto son:

- Analizar la evolución de las tecnologías de la empresa y cómo se han convertido en un factor estratégico en las empresas.

- Comprender los riesgos asociados al uso de las tecnologías y la necesidad de establecer algún tipo de control sobre las mismas.

- Entender la necesidad de un gobierno corporativo como el marco bajo el cual se gestionan los elementos relacionados con las tecnologías de información, incluidos los riesgos, y el motivo por el que deben ser responsabilidad de la Dirección de la empresa.

- Evaluar los diferentes marcos y normativas relacionados con el gobierno T.I y en concreto la norma UNE-ISO/IEC 38500, que es el referente actual para la gobernanza de las tecnologías de información. De esta comparativa, determinar cuál es el mejor marco bajo el cual implementar la norma UNE-ISO/IEC 38500.

- Diseñar un modelo, basado en el marco elegido, que permita auditar el nivel de desempeño de cada uno de los principios que conforman la norma UNE-ISO/IEC 38500, y que posibilite también la identificación de los riesgos derivados de la falta de cumplimiento de alguno de estos principios, y en el que se propongan las medidas de control oportunas.

1.3 Fases del desarrollo

Se mencionan a continuación las fases principales para el desarrollo del proyecto:

Fase de inicio, en la que se definen principalmente el objetivo y el alcance del proyecto.

Fase de análisis, hace referencia a la etapa de búsqueda de la información y definición de los requisitos que se deben cumplir. Al tratarse de un proyecto de carácter teórico, el mayor peso recae sobre estas tareas de documentación, necesaria para poder elaborar la propuesta de solución del proyecto, es decir el diseño y desarrollo de los cuestionarios de autoevaluación que permitan la realización de control y auditoría en base a la norma UNE-ISO/IEC 38500.

Fase de diseño, en esta fase se define el esquema de nuestro modelo de autoevaluación, se elaboran cada uno de los cuestionarios de evaluación y se establece la lógica del cálculo de resultados. Se incluye también el diseño de la arquitectura para la implementación de una aplicación web que de soporte a la solución propuesta: casos de uso, diagramas relacionales de bases de datos, diagramas de navegación, etc.

Una vez concluida la definición de requisitos, se puede proceder al desarrollo o codificación de la aplicación web (fase de construcción). Vinculadas a esta fase, están la fase de pruebas internas, que se irán realizando de forma paralela al desarrollo para detectar errores y verificar la funcionalidad desarrollada, y las pruebas finales, cuyo objetivo es validar la aplicación final.

Por último, se encuentran las fases de elaboración de la memoria, que comenzará una vez concluida la fase análisis, y la implantación del proyecto, que representa la entrega y presentación del proyecto.

Estas fases, serán las que se utilicen de referencia para realizar la estimación y la planificación del proyecto.

1.4 Medios empleados

En este punto se recogen los recursos necesarios y empleados para el desarrollo del proyecto.

A nivel de **hardware**, es suficiente con un único ordenador con sistema operativo Windows 8.1.

A nivel **software** se ha intentado utilizar opciones gratuitas, en algunos casos, por ejemplo, para la elaboración de la memoria se ha utilizado el paquete de Office – Word, instalado por defecto en la mayoría de los ordenadores y disponible también en cualquier ordenador de la universidad. A continuación se indica el software empleado:

- **Cacoo**. Es una herramienta online y gratuita que se ha empleado para la realización de diagramas y figuras.
- **Paquete de Microsoft Office**. Microsoft Office Word, para elaborar la memoria y lectura de documentos con extensión .doc. Y Microsoft Office PowerPoint, para la presentación del proyecto.
- **Adobe Acrobat Reader**. Permite la lectura de documentos de tipo .PDF (Portable Document Format, formato de documento portátil.)
- **Gantter**. Es una aplicación online gratuita, integrada con Google Drive, para la planificación de proyectos empresariales.

Para el desarrollo de la aplicación de autoevaluación AyCTI, se ha empleado el siguiente software:

- **JDK**, como herramienta de desarrollo de programas y aplicaciones en Java.
- **Eclipse**, como entorno de desarrollo.
- **Apache Tomcat**, como servidor de aplicaciones.
- **MySQL**, como gestor de bases de datos relacionales.

También ha sido necesaria una conexión a Internet, para la búsqueda y lectura de información en materia de gobierno y las tecnologías de información. Para la etapa de documentación también se han consultado los libros disponibles en la biblioteca.

1.5 Estructura de la memoria

Con el fin de ayudar en la lectura de la memoria a continuación se adjunta, para cada uno de los capítulos principales, un breve resumen:

Capítulo 1, **Introducción y Objetivos**. Su objetivo es proporcionar al lector el tema o idea principal a partir de la cual se desarrollado el proyecto: la tecnología de la información, su papel como factor estratégico dentro de una organización y la necesidad de gobierno de tecnología de la información. También se presentan los objetivos que se pretenden alcanzar junto con otros aspectos, como las fases de desarrollo y los medios empleados.

Capítulo 2, Estado del arte. Se analiza el concepto de tecnología de la información (T.I), su papel en la empresa y la necesidad de control interno y auditoría sobre la misma. También se señala la necesidad de un buen gobierno T.I para fomentar el funcionamiento eficiente de la tecnología de la información en una organización; incluyendo las definiciones oportunas necesarias. Por último, se mencionan los diferentes marcos y estándares que dan soporte al gobierno T.I.

Capítulo 3, Auditoría y Control según la norma UNE-ISO/IEC 38500:2013. Se plantean los problemas relacionados con el uso de la tecnología de la información y se describen cada una de las medidas propuestas que les dan solución. En este capítulo también se recogen las características funcionales del cuestionario de autoevaluación que da soporte a la solución planteada.

Capítulo 4, Planificación y presupuesto. Incluye un resumen del proyecto en relación las fases y tareas necesarias para su realización, así como un desglose de los recursos necesarios junto con su coste asociado.

Capítulo 5, Conclusiones y líneas futuras. Se describen las reflexiones a las que se ha concluido tras la realización del proyecto, valorando si los objetivos establecidos al comienzo del proyecto se han alcanzado. Se incluyen también en este capítulo las líneas futuras, es decir, aquellas ideas o mejoras que han surgido a raíz de este proyecto y que podrían realizarse sobre el mismo.

Al final del documento se encuentra el **Glosario**, que contiene las siglas o acrónimos empleados a lo largo del desarrollo de la memoria. Las **Anotaciones**, cuyo objetivo es aclarar ciertos conceptos, de carácter secundario, que se han considerado necesarios pero que debido a su naturaleza deben ir fuera del cuerpo principal de la memoria. Las **Referencias**, para indicar la fuente de la que se ha extraído un determinado párrafo o una información concreta. La **Bibliografía**, en la que se exponen todas las fuentes consultadas para el análisis y estudio de los distintos temas presentados en el proyecto. Y por último los **Anexos**, que permiten profundizar y completar los puntos del proyecto que se han considerado de mayor interés.

Capítulo 2
Estado del arte

Se describe principalmente la aplicación de la tecnología de la información (T.I), las ventajas y riesgos asociados y la necesidad de gobierno T.I.

En el apartado *2.1 Tecnología de la información y Control Interno*, se describe el concepto de las T.I y su papel en las organizaciones, así como la necesidad de control interno y su evaluación mediante la auditoría.

El apartado *2.2 Gobierno de la Tecnología de la Información*, incluye las definiciones de gobierno T.I junto con las normas y marcos que lo apoyan.

2.1 Tecnología de la Información y Control Interno

2.1.1 Tecnología de la Información y su papel en la empresa

El entorno generado en base a las tecnologías de la información ha provocado cambios tanto en la vida cotidiana, por ejemplo, mediante la incorporación a nuestro vocabulario diario de términos como email, chat, internet, etc.; como en las organizaciones, a través de la automatización de tareas, mejora de la eficiencia y reducción de costes de los procesos y donde las T.I se han convertido en un factor estratégico para la generación de valor **[1]**. Las tecnologías de información están revolucionando constantemente el panorama actual y dirigiéndolo hacia una era cada vez más digital, donde el acceso a la información en cualquier momento y a través de cualquier dispositivo se ha convertido en algo esencial, no solo para facilitar la interacción entre personas, sino también con fines educativos, de entretenimiento, científicos, comerciales. **[2] [3]**

Esta revolución afecta a los aspectos software y hardware de las tecnologías de la información. Desde el punto de vista físico se ha pasado de grandes ordenadores a ordenadores personales, y de estos a los portátiles, tabletas y teléfonos móviles, que son un excelente ejemplo representativo del avance tecnológico: cómo los dispositivos cada vez tienen mayor capacidad de procesamiento, tienen mayor autonomía y están presentes en la mayoría de nuestras actividades diarias. Hoy en día podemos encontrar procesadores u ordenadores incorporados a cualquier sistema, dispositivo o red disponible.

Desde el punto de vista del software ha permitido el acceso y la disponibilidad de una gran diversidad de productos software: bases de datos, navegadores, aplicaciones, etc. Permitiendo que de un mismo producto se puedan encontrar diferentes opciones respecto a su distribución -de pago o gratuitas-, fabricante, etc.

Respecto a las organizaciones o empresas, las tecnologías de la información han permitido entre otras, la reducción de costes de los procesos y la automatización de tareas rutinarias, de manera que las organizaciones pueden centrarse en tareas más importantes o de mayor valor. Es decir, las T.I adquieren un carácter de valor estratégico dentro de las empresas. **[10]**

2.1.1.1 Sistemas de Información y Tecnología de la Información, conceptos

La visión más intuitiva de un **Sistema de Información (S.I)** es la que se obtiene observando el flujo de la información de una empresa. Toda la información elaborada, distribuida y almacenada, junto con los procesos que la manipulan conforma el Sistema de Información de la organización.

Algunas definiciones, como las propuestas por Andreu, R., Ricart J.E. y Valor, J **[4]** contemplan el Sistema de Información como: "conjunto integrado de procesos, principalmente formales, desarrollados en un entorno usuario-computador, que, operando sobre un conjunto de datos estructurados de una organización, recopilan, procesan y

distribuyen selectivamente la información necesaria para la operatividad habitual de la organización y las actividades propias de la dirección de la misma".

También se puede considerar el Sistema de Información como un grupo de componentes o elementos relacionados entre sí, que gestionan la información con el objetivo de apoyar a la organización en las tareas de decisión, control y coordinación. **[5]**

Estos componentes requeridos los conforman los elementos físicos (el hardware), los programas o aplicaciones para el manejo de datos, y la propia información. Se tiene también en cuenta el componente humano, como aquel que proporciona la entrada de información y explota los resultados. Es decir, todo Sistema de Información realiza cuatro actividades principales **[6]**:

- Entrada de la información: en esta actividad se recogen los datos necesarios. La entrada de información puede hacerse de forma manual -a través del usuario- o de manera automática, si procede de otros sistemas.
- Almacenamiento de la información: se guarda de forma organizada la información con el objetivo de permitir que sea recuperada en cualquier momento para su uso posterior.
- Procesamiento de la información: se realizan las operaciones pertinentes de tratamiento de los datos de entrada almacenados.
- Salida de la información: la información procesada o se deriva a otro sistema o se entrega al usuario final.

Podríamos concluir entonces que la finalidad última de un Sistema de Información es la de proporcionar información en el lugar, formato y en los tiempos de respuesta establecidos, para que sirvan de base para la toma de decisiones de carácter correctivo o estratégico dentro de una empresa. Entonces, ¿cómo llevar a cabo los S.I?, mediante la Tecnología de la Información. El siguiente paso lógico será por tanto determinar qué es Tecnología de la Información (T.I):

Tecnología, según Pavez, A. **[7]**, es un "conjunto completo de conocimientos, medios y know-how organizado para obtener un resultado práctico, una innovación, bien en productos, procesos o métodos de gestión, que supongan un efecto positivo para los resultados de la empresa".

La **Información** podría ser considerada como el resultado obtenido de la interpretación de los datos que realizan las personas y la capacidad de, a partir de los mismos, realizar valoraciones y poder tomar decisiones. **[8]**

Existen dos definiciones principales, propuestas por Sáez Vacas, F. y Valle, R., que de una forma complementaria abarcan todos los aspectos que cubre y a los que da soporte la **Tecnología de la Información** (T.I):

> "Tecnologías de la información son las que se aplican en la adquisición, procesamiento, almacenamiento y diseminación de información vocal, icónica, textual o numérica." **[9]**
>
> "Se consideran tecnologías de la información aquéllas cuyo propósito es el manejo y tratamiento de la información, entendida ésta como conjunto de datos, señales o conocimientos, registrados o transportados sobre soportes físicos de muy diversos tipos. Las tecnologías de la información abarcan técnicas, dispositivos y métodos que permiten obtener, transmitir, reproducir, transformar y combinar dichos datos, señales o conocimientos." **[10]**

A partir de las dos definiciones anteriores, vamos a quedarnos con una interpretación menos rigurosa y simplificada que está contenida en ellas; la idea de que las tecnologías de la información son aquellas tecnologías que habilitan la transmisión, el tratamiento y el procesamiento de la información, y que son utilizadas en el ámbito empresarial o de los negocios para dar solución a los problemas. **[11]**

En otros casos se habla de sistemas tecnológicos de la información, que es el resultado producto de la unión de los conceptos de Tecnología de la Información y de Sistema de Información **[12].** El S.I de una organización está integrado en la estructura de sistemas de la organización, y por su parte, la T.I da soporte a la implementación y resolución de problemas que se presenten en dicho Sistema de Información.

Es decir, Tecnología de la Información son los medios, conocimientos, capacidades y técnicas que, apoyados en desarrollos tecnológicos, permiten innovar, administrar y optimizar los procesos encargados del almacenamiento, manipulación, protección y transmisión de la información. **[13]**

2.1.1.2 La Tecnología de la Información en las organizaciones

En un principio, en la etapa predigital, los cambios sobre los productos o el entorno a los que tenían que enfrentarse las organizaciones eran mínimos. Su activo clave residía en su capacidad productiva (su maquinaria, soporte logístico y de distribución, control de stock y un buen producto) y las planificaciones se realizaban para periodos estables y con previsión de crecimiento a largo plazo, lo que implicaba también que las estrategias estuvieran centradas en abarcar una mayor cuota de mercado posible, en el crecimiento y en la expansión, de manera que la tecnología no intervenía en la toma de decisiones por lo que no era considerada como un factor estratégico a tener en cuenta.

Conforme la presencia de la tecnología en las organizaciones fue incrementándose, así como el acceso y disponibilidad a la misma, para poder diferenciarse de la competencia y poder satisfacer las exigencias de los usuarios, cada vez mayores, se hizo necesario elaborar nuevas estrategias en las que se reconsideraba el papel de las Tecnologías de Información, pasando a ser considerado un factor decisivo en la consecución de los objetivos. **[14]**

Es decir, se pone de manifiesto la importancia estratégica que poseen las T.I en las organizaciones en diferentes aspectos como, la optimización de procesos, la reducción de

costes, la mejora de la calidad, y su relevancia en la competitividad entre empresas **[15].** Como consecuencia, se han generado nuevos modelos de negocio **[a]** y se ha transformado el entorno de negocio actual **[16]**:

- La información y el conocimiento no son recursos finitos y de propiedad o acceso limitado, al contrario, compartir conocimiento genera innovación y por ende mayor competencia. La tecnología es cada vez más asequible, y no puede evitarse la ingeniería inversa.
- Debido a las nuevas tecnologías las empresas pueden operar en cualquier parte, eliminado las restricciones de localización y horarios diferentes. En consecuencia, es más difícil mantener las ventajas competitivas y obtener productos únicos.
- Los cambios económicos y tecnológicos se producen a gran velocidad y pueden determinar el fracaso o éxito de un modelo de negocio si este no se adecua a ellos. Las empresas tienen que asegurar que su tecnología de información es tan buena o al menos no peor que la de sus competidores.

El valor de negocio que proporciona la T.I no se deriva de la tecnología en sí misma, ya que por sí es solo un coste. Sólo contribuye a la generación de valor cuando se acometen cambios complementarios en el propio negocio (incluidos cambios crecientemente complejos en la cultura organizativa, el modelo de negocio y el modelo operativo; en las relaciones con clientes y proveedores; en los procesos de negocio; en las prácticas de trabajo; en las competencias y habilidades del personal; en las estructuras organizativas; etc.). En última instancia, es el uso que hacen las personas de la información capturada, organizada, distribuida, visualizada y comunicada por la tecnología, lo que crea y mantiene el valor.

Las empresas que deseen sobrevivir a los cambios y tener éxito deben centrarse en preservar, proteger desarrollar y aplicar su capital intelectual. Para ello es importante que la junta directiva y los gestores estén en una posición desde la cual puedan evaluar el impacto potencial de sus negocios emergentes y de las iniciativas tecnológicas en curso. **[16]**

A modo de resumen podría decirse que las T.I tienen el siguiente impacto en las empresas **[17] [18]**:

- Modifican la estructura organizativa de las organizaciones, de manera que las funciones directivas y los procedimientos pueden verse afectados.
- Mejoran la eficiencia de las actividades definidas en la cadena de valor.
- Pueden dar lugar a nuevos negocios y alterar las relaciones con los clientes, con los proveedores y con las empresas de la competencia.
- Se eliminan barreras empresariales, mediante el uso sistemas de información automatizados.

2.1.1.2.1 Desarrollo de la estrategia T.I

Otro factor importante para garantizar el éxito de las Tecnologías de la Información dentro de su papel estratégico, es que su implantación esté alineada con la política general de la organización en la que se va a llevar a cabo, de manera que el plan estratégico que se defina tenga en cuenta todas las necesidades, a corto y largo plazo, y también los objetivos generales de la empresa. Como la Dirección es quien establece las necesidades, la estrategia y los objetivos empresariales, es indispensable su participación activa durante todas las fases de planificación, diseño e implantación de la T.I. **[19]**

Como se muestra en la Figura 1, la estrategia de negocio debería determinar la estrategia de la información; la información requerida por la organización, la de los sistemas de información -las aplicaciones que recogerán, manipularán, almacenarán y entregarán la información- y esas aplicaciones deberían ser seleccionadas de modo que las aplicaciones y los procesos de negocio estén alineados. Las necesidades de la estrategia S.I deberían determinar la estrategia tecnológica; la tecnología desplegada debería ser la más conveniente para el uso y requisitos de información de la empresa. Por supuesto, también hay retroalimentación: para determinar la estrategia de negocio, la junta directiva debe tener conciencia del tipo de información que debe ser recopilada, el tipo de aplicaciones que deben estar disponibles, y las implicaciones de infraestructura de esas aplicaciones.

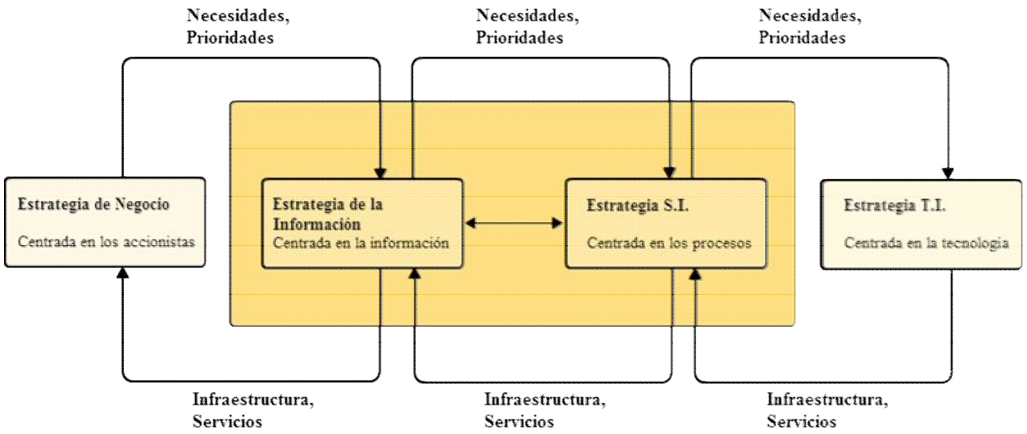

Figura 1. Desarrollo de la estrategia T.I. **[16]**

Se van a describir a continuación cada una de las etapas del desarrollo de la estrategia:

Estrategia de Negocio: algunas empresas de éxito establecen sus objetivos de negocio en base a la estrategia competitiva que han llevado a cabo para aprovechar las oportunidades, o para defender una posición, dentro de su sector profesional. La estrategia de negocio por su parte, debe tener en cuenta las propias competencias de la organización, sus puntos fuertes y debilidades respecto a la competencia, así como los activos disponibles que le permitan alcanzar sus objetivos. Esto generará una serie de requisitos para poder obtener y manipular información específica -información de productos, mercados, clientes e información de los competidores- para determinar los procesos necesarios para usar esa información eficientemente.

Estrategia de la Información: la estrategia de la información no consiste solo en identificar los activos o recursos de información necesarios y los métodos necesarios para gestionarlos. Entre sus tareas está incluida también la de saber segregar aquella información, bien demandada o facilitada, que resulte útil a la organización de la empresa para apoyar y alcanzar sus objetivos.

Estrategia SI: esta estrategia deriva de la estrategia de la información, describe a alto nivel los procesos que la organización necesita llevar a cabo y permite conocer las estrategias de arquitectura e infraestructura a desarrollar. De cara a los procesos es importante que se determinen y se desarrollen sin la influencia de procesos ya existentes.

Estrategia de las aplicaciones: su objetivo es entregar los requisitos de la estrategia de información y sus procesos de negocio. De entre todas las aplicaciones disponibles en el mercado las empresas deben establecer algún criterio de selección, teniendo en cuenta:

- La alineación con los requisitos de la estrategia de la información: elegir aquellas aplicaciones que permitan cumplir con los requisitos de información de la organización.
- El coste total por adquirir, desarrollar y mantener el software (TCO: Total Cost of Ownership/Coste Total de Propiedad).
- Elegir aquellas aplicaciones que cumplan con las condiciones de seguridad y cumplimento de la empresa.
- La aplicación elegida debe ser capaz de soportar fluctuaciones respecto al número de usuarios y requisitos de los mismos (adaptabilidad). Elegir aquellas aplicaciones que puedan tener un uso prolongando en la empresa (ROI: Return on Investment /Retorno de Inversión).

Estrategia de la Tecnología de la Información: es común que en muchas organizaciones la tecnología de la información no esté vinculada con el negocio y en ocasiones se entra en debate sobre la efectividad de las T.I.

La arquitectura T.I empresarial puede ser considerada como el conjunto de principios que determina el modo en el que la tecnología de la información y comunicación, de una organización, interactuará con sus sistemas operativos, aplicaciones y datos. A la hora de elegir una arquitectura hay que tener en cuenta los siguientes aspectos:

- Rendimiento: los sistemas de la organización deben ser robustos y capaces de mantener el nivel servicio con independencia de la demanda, sin generar cuellos de botella.
- Adaptabilidad: cuando una organización evoluciona dentro de su entorno competitivo puede necesitar adaptar y modificar sus procesos. Los sistemas deberían adaptarse a las nuevas necesidades sin coste de reconfiguración.
- Uso de software y modelos estándar: permitirá depender menos de los proveedores al no utilizar software patentado y repercutirá en un menor coste de mantenimiento de los sistemas.
- Disponibilidad de la información: en algunas organizaciones la información se almacena en silos verticales y se gestiona para obtener la respuesta a las mismas

preguntas originadas desde sistemas diferentes. Sería más óptimo que la información estuviera disponible para todos los procesos y sistemas.

Una vez decidido y aprobado el plan estratégico por la Dirección, los **pasos para su adecuado desarrollo e implementación son [16]:**

- Paso 1: la Dirección establece y acuerda la estrategia de negocio.
- Paso 2: el equipo ejecutivo identifica los requisitos de información; qué información se necesita, de dónde obtenerla y como procesarla y utilizarla.
- Paso 3: se desarrolla el S.I o requisitos de la aplicación. Para ello se describen los procesos y se identifica el software necesario que permita su desarrollo y cumplimiento.
- Paso 4: el comité de arquitectura T.I documenta la arquitectura propuesta, reflejando los principios T.I acordados y los requisitos de información y aplicaciones; este permitirá al comité tecnológico identificar el sistema operativo, hardware y las plataformas tecnológicas de comunicación necesarias.
- Paso 5: el comité tecnológico calcula los riesgos y el establecimiento de los criterios de seguridad y realiza los cambios necesarios para ajustar la estrategia T.I diseñada en conformidad con los criterios establecidos.
- Paso 6: el equipo ejecutivo asegura que las competencias y recursos han sido identificados, y que los criterios económicos y de riesgo se han cumplido. A continuación, presentan la propuesta estratégica T.I a la junta directiva para que sea aprobada.

Tras la implantación de la estrategia definida, se deberían incluir dos pasos adicionales:

- Paso 7: comprobar si las acciones tomadas en base a la estrategia continúan generando valor, y si fuera necesario, realizar las inversiones nuevas necesarias para mantener y garantizar el valor.
- Paso 8: decidir y tener claro el momento en que la inversión no es rentable.

2.1.1.2.2 Riesgos y problemas asociados al uso de la T.I

Hoy en día el número de fracasos de los denominados *proyectos T.I* es elevado. Algunos ejemplos de errores estratégicos son **[16]**:

- Las organizaciones usan menos del cincuenta por ciento de las aplicaciones software por las que están pagando una licencia.
- La mayoría del software utilizado en una aplicación está personalizado.
- El desconocimiento por parte de los responsables de este tipo de problemas. Incluyendo su falta de involucración y capacidad de gerencia.
- Cambiar la tecnología empleada cada vez que surge una nueva moda o corriente tecnológica, por el simple hecho de incorporarla a la organización aunque esta no

aporte ningún cambio o mejora a nivel de operaciones o de gestión, es ineficiente y acarrea un desembolso económico innecesario.

- El riesgo más que probable de fracaso, si las partes interesadas no se involucran en el cambio, ya que son las que poseen el conocimiento.
- Modificar la forma de hacer las cosas por la exigencia de una nueva tecnología, sin tener en cuenta si el cambio, desde el punto de vista de los sistemas de información, tiene sentido. **[20]**

Entonces, qué debe cambiar **[21]**:

- Comprender que la T.I, mediante los cambios en el negocio, pueden generar valor a la organización.
- Tener en cuenta que los beneficios no se generan de manera inmediata, ni suelen producirse en el momento ni con el margen planificado.
- Delegar a la junta directiva la toma de decisiones estratégicas y tecnológicas, y que sean por tanto los responsables de las implicaciones derivadas de tales decisiones.
- Se debe integrar la tecnología de la información como un elemento más de los procesos de la organización y de negocio.
- Realizar un análisis detallado de los cambios propuestos. Se deben conocer los resultados esperados, los mecanismos para alcanzarlos, las partes involucradas y asegurar que estas conocen y son capaces de llevar a cambio los cambios requeridos.
- Conocer cuál es el momento de dejar de invertir.

Para ayudar a identificar los problemas técnicos y de negocio vinculados con las tecnologías de la información se pueden realizar las siguientes cuatro preguntas **[21]** (Ver la Figura 2):

- ¿Las medidas y actividades que se llevan a cabo son las más adecuadas?
- ¿Los beneficios obtenidos son los esperados?
- ¿La metodología y los medios empleados son los más óptimos o eficientes?
- ¿El resultado obtenido es óptimo?

Las dos primeras hacen referencia a la capacidad estratégica y de generación beneficios que tiene la organización, y si esta permite generar o alcanzar los objetivos de negocio. La pregunta acerca del uso de las metodologías y medios, permite identificar los problemas de negocio o tecnológicos, y la necesidad de resolverlos para garantizar el éxito de las aplicaciones, programas, etc., basadas en el uso de las Tecnologías de la Información. Para terminar, la última pregunta se centra y pone de manifiesto los problemas que surgen durante la entrega de los proyectos T.I, y la capacidad de determinados grupos para solventar estos errores y proporcionar soluciones.

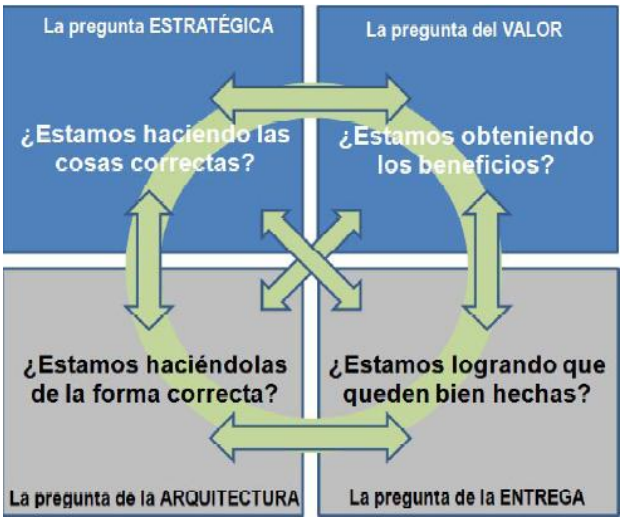

Figura 2. Las cuatro preguntas. **[21]**

Un punto clave para asegurar la efectividad de estas preguntas es realizarlas durante todo el **ciclo de vida de la T.I**. Tal y como comentan Andréu, Ricart y Valor **[4]** en la mayoría de las organizaciones la incorporación de las T.I siguen la siguiente evolución:

- Inicio: esta etapa tiene como característica principal la mecanización de un número no muy elevado de procesos, normalmente de tipo administrativo y que suelen ser muy concretos y detallados.
- Contagio: se integran e implantan en toda la organización las nuevas aplicaciones, tecnologías o desarrollos y se diseñan e implementan nuevos procesos. Además, se asignan las prioridades y los recursos necesarios.
- Control: se lleva a cabo algún tipo de medida de control con el objeto de estructurar e integrar las T.I. La junta directiva está al frente de esta etapa.
- Interdependencia entre estrategia y tecnología de la información: En esta fase la tecnología alcanza su madurez y se intenta alinear la estrategia de la organización con las T.I. Aunque como recomendación se sugiere definir la estrategia T.I en las primeras etapas, para poder realizar lo antes posible los ajustes y cambios necesarios para corregir posibles desviaciones.

2.1.2 Control Interno y Auditoría Informática

Como se ha expuesto en los puntos anteriores, la información junto con la tecnología de información son recursos estratégicos en las organizaciones y por tanto deberían ser protegidos, ya que constituyen la base de casi todas las decisiones que se toman.

No disponer de la información exacta y adecuada, en el formato y momento adecuado puede ocasionar entre otros, duplicidad del trabajo, retrasos en la toma de decisiones críticas y sanciones de las entidades reguladoras. Para asegurar el cumplimiento de estas cuestiones se deberán desarrollar controles internos de carácter informático, que ayudarán

a satisfacer y a cumplir las normativas legales y a garantizar que los sistemas y las tecnologías funcionan según lo establecido y esperado. **[22]**

Son muchos los escándalos y fracasos relacionados con el uso de las tecnologías de la información que han salido a la luz. Esto ha provocado una mayor sensibilización de la necesidad de control interno y de optimizar los mecanismos de control.

2.1.2.1 El problema con la T.I y la necesidad de auditoría y control interno

El uso de la información y de la tecnología de la información está generalizado, ambos son esenciales en las operaciones y procesos organizativos y conforman el núcleo estratégico de la mayoría de las empresas. Por otra parte, suele ser problemática, ya que con frecuencia se producen errores y sus consecuencias tienen un alto impacto. Salvo que la organización tenga en cuenta la necesidad de asegurar la disponibilidad, integridad y confidencialidad de su información y de la tecnología de información, mediante la implantación de mecanismos de control, será vulnerable. Algunos de estos problemas son riesgos inherentes al propio uso de la T.I y son debidos a **[22]:**

- Uso de sistemas antiguos.
- Falta de gestión del riesgo.
- Ausencia de controles de los S.I.

Mencionemos algunos de estos fracasos T.I a modo de ejemplo:

- Cuando el Royal Bank of Canadá llevó a cabo las tareas de mantenimiento de las aplicaciones de contabilidad, provocó que durante un periodo de cinco días no se pudieran obtener los saldos de los clientes.
- Una compañía farmacéutica perdió más del 27% de su valor de mercado en bolsa cuando al implantar su nuevo sistema de planificación de recursos, no pudo generar los informes obligatorios ni realizar los cuadres de cuentas.

Esta pequeña muestra evidencia que este tipo fallos tienen un gran impacto en aquellas organizaciones dependientes de la tecnología de la información, tanto a nivel operativo, daños legales o en la reputación de la empresa. **[23]**

Estas tareas de identificación de riesgos y vulnerabilidades no corresponden al departamento T.I sino que forman parte de las tareas de gestión de la información. Los directores, ejecutivos y gestores de cualquier organización, independientemente de su tamaño, tienen que entender cómo asegurar sus inversiones.

La dirección eficaz tanto del riesgo de la información como de la tecnología de la información tiene dos componentes principales. El primero se relaciona con el uso de la tecnología de la información como factor estratégico en las empresas para alcanzar sus objetivos de negocio. Este proceso suele implicar una inversión significativa de recursos por lo que hay interés, por parte de las partes implicadas, en que los despliegues e implantaciones de proyectos finalicen con éxito. Este interés debería reflejarse en una transparencia sobre la planificación y gestión de los mismos, y en la identificación y

control de los riesgos. El segundo componente es la forma en la que se gestionan los riegos asociados con los activos de la información.

Es decir, nos encontramos en una fase de madurez de las organizaciones en la que el control y la mejora de las actividades se han convertido en necesidades básicas y prioritarias. Los siguientes factores demuestran la necesidad de control y de la auditoría en las organizaciones **[24]**:

Costes ocasionados por pérdida de datos: los datos son un factor crítico en las organizaciones para garantizar el funcionamiento correcto y su operatividad.

La solución pasaría por realizar copias de respaldo o de seguridad y controles de los mismos.

Adopción de decisiones poco adecuadas: los datos deben ser lo más exactos posibles, tanto para las decisiones a corto como a largo plazo y sobre todo para aquellas relacionadas con el control y las operaciones. Cualquier variación en los datos puede implicar pérdidas de costes y en los resultados de los procesos.

Como medida se propone que el grado de evaluación y control que se realice sobre los datos esté directamente relacionado con la criticidad de los mismos.

Fraudes o delitos: son todas aquellas actividades ilícitas asociadas con de la tecnología que tiene como objetivo el daño de terceros o el beneficio propio del causante.

Para evitarlos se debe en primer lugar, proteger los activos, aplicar los protocolos y normativas y conocer la legislación vigente.

Valor de los recursos: hay que tener en cuenta el impacto a nivel operativo que puede provocar el mal funcionamiento o la ruptura del hardware o del software. También hay que considerar la pérdida de recursos humanos, sobre todo si están bien cualificados.

Hay que anticiparse a las posibles bajas y minimizar su impacto, mediante la duplicidad de sistemas, copias de seguridad, formación del personal, etc.

Coste de los errores informáticos: debido a la criticidad de las tareas que llevan a cabo los sistemas informáticos, los costes asociados cuando se produce un error son muy elevados.

Se pueden evitar errores si se opera según las normas, mediante la realización de pruebas y revisiones.

Privacidad: se debe garantizar la privacidad de los datos personales y los datos de las organizaciones para asegurar que los estos sólo sean utilizados para el propósito para el que han sido recopilados.

Hay que limitar el acceso a los datos privados solo bajo la autorización correspondiente.

Control del uso de las tecnologías de la información: hay que establecer las responsabilidades y las limitaciones correspondientes.

° Detallar las situaciones y casos en los que está autorizada o debe prohibirse su uso, por ejemplo, en intervenciones médicas, en la conducción de vehículos

° Señalar quién es responsable si se produce un fallo: los desarrolladores de las T.I, las personas que lo usan…

Este aspecto se debe detallar e incluir en los contratos y estar contemplando en la normativa.

2.1.2.2 Control Interno y Auditoría Informática

2.1.2.2.1 Control Interno Informático

El Control Interno es el encargado de controlar las distintas actividades y procesos, en el ámbito de una organización, para garantizar que se realizan en base a la normativa, los estándares, requisitos establecidos; y de asegurar que son válidas y correctas**. [25]**

Otra definición es la sugerida por Platttini, Mario G., para el que el control interno es toda actividad manual o automática que permita la detección, prevención y solución de aquellos errores que pueden alterar o interrumpir el funcionamiento correcto de un sistema y por tanto afectar al logro de los objetivos. **[26]**

Los principales objetivos del Control Interno son **[26]**:

- Garantizar el cumplimiento de todas las actividades según las normas y procedimientos determinados.
- Proporcionar asesoramiento sobre el conocimiento de las distintas normativas.
- Servir de apoyo a la Auditoría Informática, interna y externa.
- Llevar a cabo el desarrollo, implantación y ejecución de los controles y mecanismos necesarios para poder evaluar el grado de cumplimiento de los servicios informáticos.
- Controlar todas las actividades que se realizan en los distintos sistemas y entornos informáticos.

Los objetivos pueden clasificarse en las siguientes categorías **[27]:**

- Controles preventivos: intentan evitar errores o determinados hechos, por ejemplo, evitar el acceso a datos protegidos mediante el software correspondiente.
- Controles detectivos: son los encargados de solventar y detectar los errores que las medidas preventivas no han podido evitar.
- Controles correctivos: para salvar errores y situaciones producidas por omisiones.

En ocasiones se incluyen también los controles de tipo directivos y los de recuperación. Los primeros establecen las pautas para el desarrollo de nuevos controles. Los segundos facilitan y restauran la normalidad ante una interrupción o un error. **[28]**

2.1.2.2.2 Auditoría Informática

La Auditoría Informática se encarga de recopilar y analizar evidencias con el propósito de saber si un determinado sistema asegura la integridad de los datos, protege los activos, hace un uso eficiente de los recursos y satisface los objetivos de la organización. **[26]**

Aunque a veces se asocia auditoría informática con auditoría de la seguridad, la auditoría informática puede incluir otras áreas. A modo de descripción podemos decir que la auditoría informática incluye la supervisión, el estudio y la evaluación objetiva e imparcial, por parte de las personas que la llevan a cabo, sobre **[28]:**

- el **entorno informático** de una entidad y las áreas que lo conforman: aplicaciones, equipos, sistemas operativos…
- los estándares, **políticas y procedimientos** vigentes en la entidad y su grado de cumplimiento. Se incluyen también los presupuestos, las metas y la normativa legal que se puede aplicar.
- el **grado de satisfacción** las partes implicadas.
- los **controles** implantados en la entidad.
- el análisis de **riesgos** probables.

2.1.2.2.3 Control Interno y Auditoría Informática

A modo de resumen podríamos decir entonces que, el Control Interno Informático tiene como finalidad establecer y diseñar los controles que deben realizarse, de forma periódica, en cada una de las funciones o áreas informáticas. Por su parte, la tarea del auditor informático (externo o interno) será la de revisar los controles internos definidos y asegurar que se cumple la normativa en base al nivel de riesgo. **[29]**

En la siguiente figura (Figura 3) se establecen los objetivos comunes y diferencias entre ambas:

	CONTROL INTERNO INFORMÁTICO	AUDITORÍA INFORMÁTICA
SEMEJANZAS	* Conocimientos específicos de Tecnología de la Información. * Verificación del cumplimiento de los controles internos, los procedimientos y la normativa definida por la Dirección.	
DIFERENCIAS	* Análisis diario de los controles. * Reporta a la Dirección del Departamento de Informática. * Sólo el personal interno. * El alcance de sus funciones es únicamente para el Departamento de Informática.	* Se analiza un proceso a actividad determinada. * Reporta a la Dirección General de la Organización. * Personal interno y/o externo. * Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización.

Figura 3. Similitudes y diferencias entre control interno y auditoría informática. **[26]**

2.2 Gobierno de la Tecnología de la Información

2.2.1 Conceptos y definición de Gobierno

A medida que las organizaciones crecen, la manera en la que son gobernadas adquiere mayor importancia y aspectos como el control, las responsabilidades, los objetivos, y el valor que generan se convierten en aspectos importantes a definir y a tener en cuenta para un correcto gobierno.

El interés en mejorar el gobierno corporativo está relacionado entonces con el desarrollo de medidas que satisfagan a todas las partes implicadas y que estén afectadas por las actividades de la organización.

Posteriormente, el gobierno corporativo da lugar al gobierno de T.I, mediante la elaboración y mejora de sistemas que permiten llevar a cabo las mejores prácticas y desarrollar los procesos más eficientes en el ámbito de las tecnologías de la información. **[65].**

2.2.1.1 Definición de Gobierno Corporativo y Gobierno de T.I

El gobierno corporativo es quien tiene la capacidad para incrementar el valor, el crecimiento de las organizaciones y conseguir un mayor respaldo de los inversores. Es decir, son los responsables de cómo se gestiona el negocio y se controlan los riesgos con el fin de conseguir las metas de la organización y sobrevivir a entornos cambiantes de mercado **[30];** El gobierno corporativo debe también basarse en los siguientes principios elementales **[31]:**

- Definir la misión, la visión, los objetivos y los valores de la entidad.
- Diseñar una estructura de la organización lo menos rígida posible.
- Definir la relación y dependencia de los componentes de la organización.
- Elaborar e implantar los sistemas de monitorización y de control.

El Cadbury Report, por su parte, describe el papel del gobierno corporativo como el medio mediante el cual las actividades de la empresa son controladas y dirigidas, papel que recae sobre el Consejo. Sus responsabilidades incluyen, determinar los objetivos de la empresa, liderarla para alcanzar esas metas y supervisar la gestión del negocio. Todas las acciones que tomen tienen que realizarse conforme a las regulaciones y leyes, y deben contar con la aprobación de las partes interesadas. **[32]**

En relación a las tecnologías de la información, debido al papel crítico y clave que ha adquirido en los últimos años en la consecución de los objetivos de la empresa, se hace necesaria la existencia de un gobierno de las tecnologías de la información que las dirija y regule de la forma más eficiente posible. El gobierno T.I debe garantizar el uso óptimo de las tecnologías de la información, proporcionar los mecanismos de control apropiados,

analizar la viabilidad de los proyectos T.I y el coste de las inversiones para poder generar valor al negocio. **[31]**

Según el ITGI **[c]** debe cumplir los siguientes objetivos **[31]:**

- Especificar y dirigir las estrategias de la organización.
- Garantizar el cumplimiento de los objetivos.
- Realizar una gestión adecuada de los riesgos.
- Verificar el uso responsable de los recursos.

Otras acepciones más recientes de gobierno T.I son las propuestas por la norma UNE-ISO/IEC 38500:2013 *Gobernanza corporativa de la tecnología de la información*, que contempla el gobierno de las T.I como "el sistema que gestiona el uso, actual y futuro, de la T.I"; y la propuesta por ISACA **[d]**, donde el gobierno de las T.I es "una función de gobierno, que está formado por el gobierno de negocio de las T.I (garantiza que las T.I permitan y soporten el desarrollo la estrategia de la organización) y por el gobierno funcional de las T.I (garantiza que la función de T.I se lleva a cabo de manera eficaz y de forma eficiente)". **[33]**

La correspondencia entre de gobierno T.I y el corporativo podría establecerse indicando que el gobierno corporativo constituye la base del gobierno T.I, en cambio este es un elemento estratégico clave producto del proceso de gobierno corporativo. **[31]**

2.2.1.2 Diferencia entre gobierno y gestión de la T.I

En la industria de las T.I suele haber confusión entre los conceptos de *gobernanza* y *gestión*. Pero, mientras que hay una línea clara para explicar qué es *gobernanza,* para gestión no la hay y en ocasiones, las definiciones existentes no tienen la suficiente separación contextual.

Al igual que en el caso de gobierno T.I, la norma UNE-ISO/IEC 38500:2013 consideró esencial incluir también una definición para la gestión: "son los procesos y los controles indispensables para lograr los objetivos estratégicos establecidos por la dirección de gobierno de la entidad".

Podríamos señalar que la gestión de las tecnologías de información se centra en las operaciones internas de la T.I en el día a día, mientras que el gobierno de las T.I atiende a las demandas externas de los clientes tanto presentes como futuras. De manera que, la gestión se centra en la implementación y gestión de las estrategias diarias, y el gobierno se encarga de fijar y elaborar esas estrategias, alineándolas con la cultura y la política empresariales. **[33]**

Para otros autores, el gobierno de la organización hace referencia a los responsables y a la tarea de gestión y coordinación de las actividades empresariales, y el gobierno corporativo al consejo o a la junta directiva. El gobierno de las T.I está enfocado en la utilización de la tecnología para poder alcanzar los objetivos especificados por la

Dirección, es decir, el gobierno corporativo engloba ciertas facetas del gobierno de la T.I. **[33]**

Por último, la definición aportada por Mark Toomey, para quien el gobierno es ejercido por el cuerpo de gobierno y lo conforma el consejo de administración, mientras que la gestión la relaciona con el Director o Gerente general. **[23]**

En la siguiente figura (Figura 4) se representa de forma esquemática y a modo de resumen la comparación entre gobierno y gestión T.I.

	Gobierno T.I	**Gestión T.I**
Definición	Se centra en los seis principios: • Responsabilidad • Estrategia • Adquisición • Rendimiento • Conformidad • Factor humano Y en tres funciones: • Evaluar • Dirigir • Monitorizar	Ejecuta las políticas, estrategias y planes aprobados por el Gobierno.
	Alinea el plan de las T.I con el plan de negocio de la empresa.	Gestiona los distintos servicios y operaciones de las áreas para cumplir los objetivos definidos.
Quién lo conforma	El consejo de administración.	La dirección general y los directores de departamento o área.
Tareas	Define el plan estratégico.	
	Aprueba el plan estratégico.	
	Aprueba las políticas y reglas de la empresa.	Define o propone las políticas y reglas de la empresa.
	Obtiene la información para monitorizar y evaluar la ejecución de políticas, estrategias, e incluso el esquema de toma de decisiones.	Realiza la evaluación.

Figura 4. Comparativa Gobierno y Gestión T.I**. [33]**

Como se puede deducir, para conseguir que los recursos T.I sean los más eficientes posibles y maximizar el valor que aportan al negocio, tanto la gestión como el gobierno T.I deberían funcionar correctamente. **[34]**

En resumen, el cuerpo de gobierno junto con el de gestión elaboran la estrategia empresarial. Por un lado, el gobierno establece las pautas de gerencia y monitoriza el desempeño de la entidad; y la gestión T.I, desarrolla las capacidades de negocio y gestiona los recursos tecnológicos para garantizar el cumplimiento de los objetivos establecidos en la estrategia de negocio tanto en plazos, costes como en resultados **[35]:**

Figura 5. El rol de gobernanza corporativa. **[35]**

2.2.1.3 Gobierno T.I, áreas de enfoque

Las decisiones relativas a Gobierno T.I que deben tomarse están clasificadas en las siguientes áreas **[36]:**

- **Objetivos**. Engloban las decisiones relativas a la estrategia, normativas, procedimientos T.I y los objetivos de control que deben ser medidos. Algunos ejemplos de cuestiones sobre las que hay que decidir en relación a los objetivos pueden ser:
  - Políticas y normas para guiar el uso de las T.I.
  - Los objetivos de control, que son usados para monitorizar el comportamiento de los procesos T.I.

- **Procesos**. Hacen referencia a las tareas de procesos de gestión, desarrollo e implantación de procesos T.I, y la gestión de recursos T.I. Por ejemplo:
  - Diseñar los flujos de los procesos: las entradas, salidas, valores esperados, etc.
  - Documentar y acordar los pasos necesarios para la implantación de los procesos y la gestión de errores.

- **Personas.** Describe la estructura organizacional, las relaciones entre las personas y la asignación de responsabilidades y roles. Las organizaciones utilizan un número determinado de estructuras alternativas para organizar sus T.I, incluyendo, por ejemplo, comités de T.I, reubicación y rotación de trabajos. Algunos ejemplos de las cuestiones sobre las que hay que decidir en esta área, son:
  - Los roles y su asignación, de manera que quede claro su papel su relación con la T.I.
  - Describir las tareas de cada rol.

- **Tecnologías**. Incluyen la parte hardware y el software. El gobierno T.I tiene que asegurar que las inversiones en T.I generen el valor deseado para el negocio y mitigar los riesgos asociados a las mismas. Algunas de las decisiones tecnológicas que hay que tomar son:
  - Las relacionadas con la infraestructura tecnológica.
  - Sobre las aplicaciones, por ejemplo, los sistemas operativos y los sistemas CRM (gestión de relaciones con el cliente),
  - Sobre el almacenamiento, estructura y uso de la información.

A su vez, el ITGI establece cinco áreas de enfoque principales en las que se pueden agrupar las actividades de gobierno T.I **[37] [38]**:

Figura 6. Áreas de enfoque del Gobierno T.I. **[c]**

Alineación estratégica: se valora si los procesos, las operaciones y las inversiones T.I están alineados con la estrategia y los objetivos empresariales, lo que permitiría la creación de valor para el negocio.

Entrega de valor: el objetivo es alinear la estructura T.I con la del negocio, para garantizar que tanto los servicios como los procesos y los productos cumplan con las especificaciones requeridas. En este caso las T.I permiten reducir costes y optimizar los tiempos de entrega.

Administración de riesgos: abarca las diferentes etapas de la gestión de riesgos: identificación, evaluación, implantación de las distintas medidas de control, así como el diseño y desarrollo de las medidas correctivas.

Administración de recursos: hace referencia a la gestión eficiente de los distintos recursos T.I, como pueden ser los datos, los programas o aplicaciones, etc.

Medición del desempeño: se llevan a cabo las tareas de seguimiento y control, medición y evaluación de todas las áreas T.I. Los resultados, pueden evidenciar puntos críticos que pueden afectar al desempeño, y en base a ellos tomar las medidas oportunas para el

correcto gobierno de los riesgos, de los recursos, analizar si la entidad se está desviando en relación a lo establecido en su plan estratégico, etc.

2.2.2 Marcos de Gobierno T.I

En puntos anteriores se ha analizado el papel estratégico, cada vez más relevante, de la Tecnología de la Información en las organizaciones. Como resultado quedaba patente la necesidad de la existencia de algún marco o normativa que regulara su gobierno, el gobierno T.I. **[39]**

Un marco podría considerarse como aquellos métodos y prácticas que sirven a las organizaciones de modelo de referencia para especificar **[40]:**

- Los procesos T.I: su funcionalidad, su nivel de criticidad, las partes implicadas y su responsabilidad.
- Los recursos: permite gestionar los recursos T.I de forma eficiente.
- Los controles: propone medidas de control en base a la experiencia de las mejores prácticas.
- La normativa: facilita el cumplimiento y adopción de la normativa regulatoria.

En ocasiones los marcos suelen ser complementarios, pueden hacer alusión a los mismos aspectos o plantear enfoques diferentes sin determinar cómo se integran con otros modelos. No obstante, a pesar de los posibles inconvenientes siempre será mejor trabajar con ellos, pues permiten a las organizaciones **[39]**: garantizar la consecución de objetivos, estimar de forma adecuada los recursos necesarios, minimizar los riesgos, cumplir con la normativa aplicable, monitorizar y verificar el grado de satisfacción y cumplimento de las T.I al negocio. **[41]**

Se detallan, a continuación, de forma breve algunos de los marcos más reconocidos:

COBIT (Control Objectives for Information and related Technology – Objetivos de Control para Información y Tecnologías Relacionadas).

Este marco de trabajo fue creado por el ITGI. Es uno de los marcos con mayor aprobación y aceptación para el control, el uso de la tecnología de la información y los riesgos asociados. Incluye una guía de gestión para el control y medición de las T.I a través de una serie de procesos que tiene identificados y definidos **[16]**. La versión actual, a fecha de este proyecto, es COBIT 5.

ITIL (IT Infraestructure Library - Biblioteca de Infraestructura de Tecnologías de Información).

Podría considerarse el marco referente para la gestión de servicios. ITIL establece una serie de recomendaciones o buenas prácticas para la tecnología de la información en el ámbito de desarrollo, gestión y servicios. **[42]**

En la tercera versión, los servicios están catalogados por fases del ciclo de vida del servicio: Estrategia del servicio, Diseño, Transición, Operación y Continuidad del servicio. **[43]**

PMBoK (Project Management Body of Knowledge **-** Fundamentos para la Dirección de Proyectos).

PMBoK, es una guía llevada a cabo por el Project Management Institute, en la que se describen los principios de gestión de proyectos **[44]**. Esta guía propone un conjunto de nueve áreas de conocimiento, que son comunes a la mayoría de los proyectos, y clasifica los procesos en cinco grupos: inicio, planificación, ejecución, supervisión y control, y cierre. **[45]**

PRINCE2 (Projects in Controlled Environments – Proyectos en Ambientes Controlados).

Más que un conjunto de buenas prácticas, PRINCE2 es una metodología de gestión de proyectos que cubre: la calidad, el cambio, la organización del proyecto, la planificación, el riesgo y el progreso del proyecto.

Cada proyecto está compuesto por un conjunto de fases manejables, lo que permite un mayor control a nivel de planificación y de recursos. Además, esta metodología puede aplicarse en proyectos de toda clase. **[46]**

CMMi: (Capacity Maturity Model Integrated – Integración de Modelos de Madurez de Capacidades).

Es un marco de mejora del rendimiento, que permite medir el grado de madurez, en un nivel de uno a cinco, de una organización en relación a las mejores prácticas de gestión y de desarrollo.

En base a los objetivos de negocio de una organización, CMMi proporciona un conjunto de prácticas para la mejora de los procesos. Estas no están restringidas al nivel organizativo, también se contemplan tareas de mejora de rendimiento de otras áreas, hasta lograr un retorno positivo de la inversión. **[47]**

Val IT

Val IT es una propuesta del ITIG. Define un conjunto de prácticas y guías para ayudar a las empresas, en concreto a la junta directiva, a maximizar el valor obtenido en las inversiones relacionadas con la tecnología de la información:

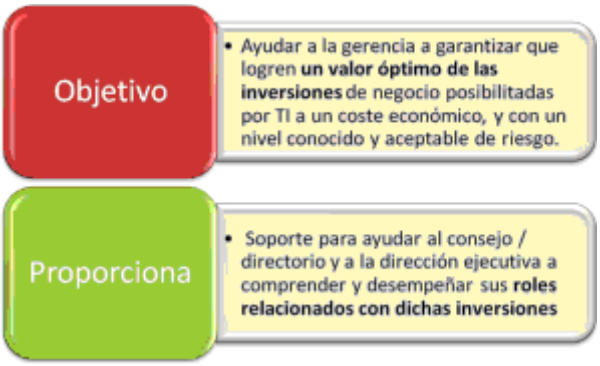

Figura 7. Definición de Val IT. **[48]**

Val IT complementa a COBIT, ya que mientras que el primer marco está enfocado en cuestiones relativas a la inversión y a los beneficios, el segundo se centra en la gestión. **[48]**

Dada la importancia que tiene la arquitectura empresarial **[e]** como factor clave para lograr un gobierno T.I eficiente, existen marcos que se centran en ella: TOGAF, Zachman, DoDAF, FEAF. Los dos marcos más reconocidos son Zachman y TOGAF, y se describen a continuación **[49]:**

TOGAF (The Open Group Architecture Framework - Esquema de Arquitectura del Open Group).

Este marco de trabajo, que se basa en un modelo repetitivo de procesos **[50]**, está enfocado en la arquitectura de la información y en proporcionar orientación sobre sus distintas etapas: planificación, diseño, implementación y gobierno. A su vez, cada arquitectura está dividida en cuatro niveles: Negocio, Datos, Aplicaciones y Tecnología. **[51]**

Zachman

Zachman clasifica los elementos más relevantes de las empresas para su gestión, a través de una plantilla bidimensional. Cada columna representa un aspecto de la empresa definido a través de preguntas: ¿Qué?, ¿Cómo?, ¿Dónde?, ¿Quién?, ¿Cuándo?, y ¿Por qué? Mientras que las filas representan los roles involucrados en la organización. Cada celda, formada por el par columna-fila, describe por tanto un aspecto de la empresa según un punto de vista determinado. **[52]**

2.2.3 Normas y estándares para el Gobierno T.I

2.2.3.1 Normas y estándares

La evolución de las Tecnologías de la Información, así como su incorporación y su papel dentro de las empresas, provocó un nuevo enfoque de la normativa hacia una visión de gestión y el desarrollo de numerosos marcos y normas ISO, con el fin de controlar y conseguir un uso eficiente de las Tecnologías de la Información.

Los marcos proponen e incluyen un conjunto de prácticas, pero no indican qué requisitos son obligatorios para cada nivel. Esto permite a las empresas aplicar al inicio las prácticas más básicas, pues al principio no cuentan con los recursos adecuados y necesarios para llevar a cabo todos los procesos del marco, y poder ampliarlas a lo largo del tiempo. **[53]**

Un estándar sí describe los requisitos y los controles que la entidad debe satisfacer para cumplir con esa normativa concreta y ser certificada. Los estándares tienen carácter voluntario, y es decisión de la empresa determinar el cumplirlos o no. **[53]**

En la Figura 8 se resumen las principales características de ambos:

Marco de referencia	Estándar
Describe mejores prácticas.	Define una manera repetible de hacer algo previo acuerdo.
Proporciona guías y sugerencias.	Define una especificación formal.
Da soporte a los esfuerzos de una organización para diseña y mejorar de manera continua los procesos.	Prescribe un conjunto mínimo de prácticas que la organización debe poner en práctica para asegurar la calidad de los procesos.
Carece de controles obligatorios necesarios para que una organización demuestre conformidad.	Lista controles obligatorios que la organización debe mostrar como evidencia para ser certificada.

Figura 8. Características de marcos de referencia y estándares. **[53]**

A nivel mundial, el sistema de normalización lo constituyen ISO, UIT (Unión Internacional de Telecomunicaciones) e IEC (Comisión Electrotécnica Internacional). JTC 1 **[f]** es la fuente actual de referencia, en el ámbito de las T.I, para abordar las iniciativas de normalización en el ámbito T.I.

En España el apogeo de la tecnología de la información tuvo lugar en la década de los noventa y AENOR **[g]** fue la encargada de afrontar esta nueva demanda, mediante la hoja de ruta para la gestión y gobierno TIC (Tecnología de la Información y Comunicaciones). Lo que propone es integrar la T.I como un elemento más de la empresa, dirigida a los objetivos de negocio. **[39]**

El modelo propuesto por AENOR (ver Figura 9) tiene dos áreas principales, la parte del gobierno de las TIC y la de gestión, que corresponden a las normas UNE-ISO 22301:2015, UNE-ISO/IEC 38500:2013. **[i]**

A su vez, el área de gestión está compuesta por la gestión de servicios T.I (SGSTI) y la seguridad de la información (SGSI): UNE-ISO/IEC 20000-1:2011 y UNE-ISO/IEC 27001:2014, respectivamente. La primera norma permite alcanzar la calidad en los servicios teniendo en cuenta los objetivos de la organización; y la segunda, gestionar los riegos. **[70]**

La otra área de la gestión agrupa la normativa relacionada con el desarrollo software: evaluación y madurez (SPICE ISO 15504: 2004), procesos del ciclo de vida (ISO 12207:2008); y la norma para la gestión de activos (UNE-ISO/lEC 19770-1:2008 *Tecnología de la Información. Gestión de activos de software (SAM). Parte 1: Procesos).*

El modelo se completa con las siguientes normativas: ISO/IEC 29110:2011, sobre el ciclo de vida de empresas pequeñas, ISO/IEC 25000:2014 e ISO/IEC/IEEE 29119:2013, normas de calidad de producto y pruebas software. **[70]**

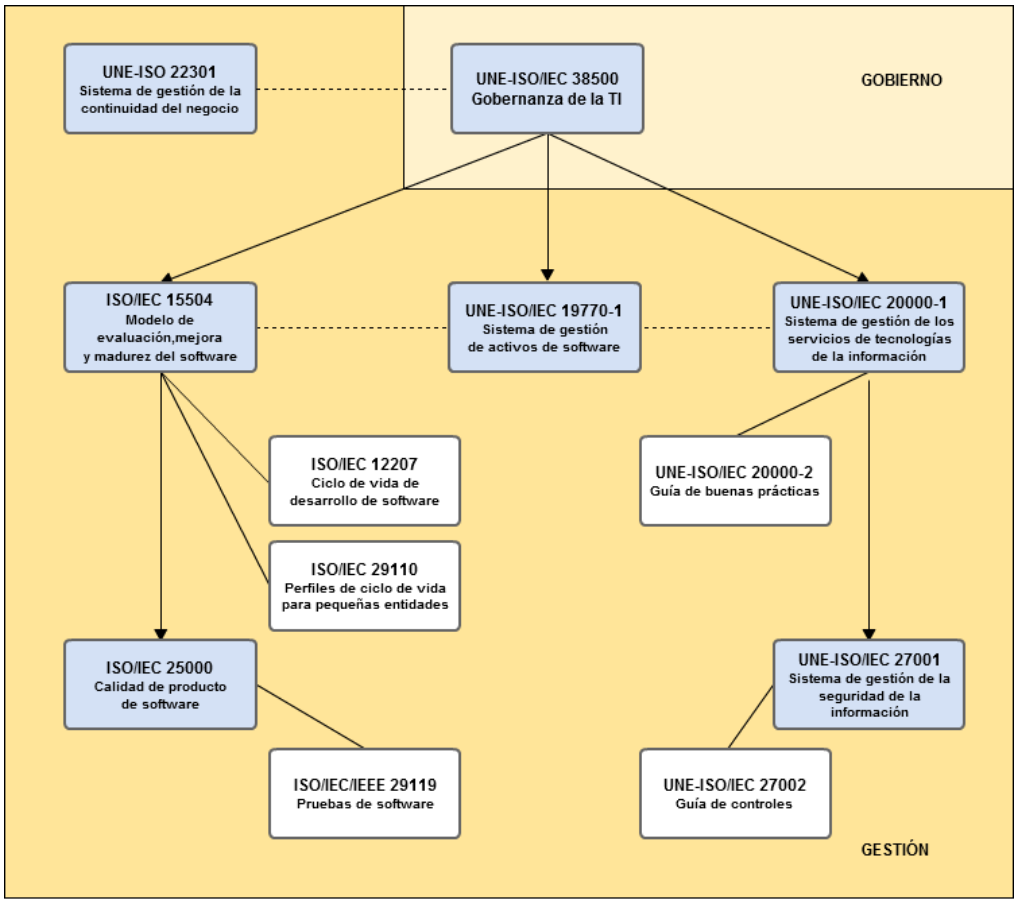

Figura 9. Modelo ampliado de AENOR para las TIC. **[33]**

Por tanto, las empresas actualmente cuentan con un conjunto de normas de reconocimiento internacional para abordar la organización de las tecnologías de la información. Estas normas están basadas en el esquema PDCA (Plan Do Check Act /

Planificar Hacer Verificar y Actuar) **[h]** lo que les permite su integración con otros modelos, por ejemplo, el modelo 9000 relativo a la gestión de calidad.

Se definen a continuación otra serie de normas que completa el modelo descrito **[33]:**

UNE-ISO/IEC 90003: 2005 *Ingeniería del software. Guía de aplicación de la ISO 0001:2000 al software*, permite extender el sistema de gestión de la calidad que posee la organización a las tecnologías de la información.

La serie ISO/IEC 15408:2009 *Tecnología de la Información - Técnicas de Sistemas - Criterios de evaluación para la seguridad de las T.I*, para determinar la evaluación y los controles relativos a la seguridad de las T.I.

ISO/IEC TR 24766:2009 *Tecnología de la Información – Ingeniería de sistemas y software – guía para las capacidades de la herramienta de ingeniería de requisitos*, describen las características de las herramientas de gestión de requisitos.

ISO/IEC 24773:2008 *Ingeniería software – Certificación profesional de ingeniería – Comparación del Marco*, indica las pautas para aquellas personas vinculadas con la T.I que quieran certificarse.

ISO 31000:2009 *Gestión de Riesgos – Principios y guías,* establece modelos para la gestión de los riesgos.

2.2.3.2 Principales características de los modelos de gestión

A continuación, para completar el punto anterior se van a describir de forma breve la normativa mencionada para el Gobierno y la Gestión T.I **[33]:**

UNE-ISO/IEC 38500:2013 *Gobernanza corporativa de la Tecnología de la Información*.

Es el estándar internacional para el gobierno corporativo relacionado con las tecnologías de la información. Proporciona una vista simple y única del rol de la Dirección en las tareas de dirigir, evaluar y ejecutar las distintas actividades T.I de la organización. **[54]**

La norma se publicó en el año 2008 en base a la norma australiana AS8015: 2005, y está reestructurada en dos partes:

- ISO/IEC 38501 Gobierno corporativo de las Tecnologías de la Información (T.I). Directrices de implantación.
- ISO/IEC 38502 Gobierno corporativo de las Tecnologías de la Información (TI). Modelo y marco de referencia.

UNE-ISO 22301:2015 *Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012).* **[55]**

Esta norma anula a la norma UNE 71599 *Gestión de la continuidad del negocio* y sustituye a la Norma Internacional ISO 22301:2012. Engloba todas las actividades necesarias para proteger a la entidad contra incidentes que puedan afectar a la continuidad del negocio y a establecer las medidas preventivas y correctivas correspondientes.

La norma establece las bases para que cada organización, independientemente de su tamaño y tipo, diseñe su Sistema de Gestión de la Continuidad del Negocio (SGCN) en base a los requisitos legales, de sus procesos, de las partes involucradas y del tamaño y estructura de la organización.

UNE-ISO/IEC 20000-1:2011 *Tecnología de la Información. Gestión del servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio*.

Es parte de la serie ISO/IEC 20000. Especifica los requisitos obligatorios que debe cumplir el proveedor de servicios de T.I para mantener el Sistema de Gestión de Servicio, de manera que queden cubiertos todos los requisitos actuales, así como las necesidades futuras. **[42]**

UNE-ISO/IEC 27001:2014 *Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.*

La piedra angular del sistema ISO 27001 es la gestión de riesgos y el establecimiento de controles para los procesos y servicios T.I, para proteger la información de manera permanente. **[42]**

En las últimas versiones se ha incorporado el concepto de *Estructura de Alto Nivel,* bajo el Anexo SL, que posibilita la integración de la norma con otros sistemas de una manera más sencilla. Otras novedades que incorpora son, el refuerzo por la mejora continua, fundamentándose en el ciclo Deming o PDCA; y destacar el papel de las partes interesadas en el cumplimiento de los objetivos de seguridad de la información. **[56]**

SPICE ISO/IEC 15504:2004 *Determinación de la Capacidad de Mejora del Proceso de Software/ Software Process Improvement and Capability Determination.* **[57]**

La norma ISO/IEC 15504:2004 tiene como objetivo evaluar los procesos para detectar los puntos críticos y proponer una serie de medidas para solventarlos y conseguir también mejorar su capacidad.

Está compuesta por varias partes, de las cuales las más importantes son:

- parte normativa: establece los requisitos, aspectos y consideraciones mínimas del modelo de evaluación y mejora.

- parte informativa: aquella que las organizaciones pueden utilizar como guía para aplicar la parte normativa.

ISO/IEC 12207:2008 *Sistemas e ingeniería de software - procesos de ciclo de vida de Software.*

La norma clasifica los procesos que cubren el ciclo de vida de un sistema software en siete grupos, donde cada uno cuenta además con dos subdivisiones: el contexto del sistema y contexto del software.

Cada proceso incluido en los grupos se define en base a sus objetivos y al conjunto de tareas que hay que realizar para alcanzar esos resultados deseados. De manera que cada proceso constituye un modelo de referencia. **[58]**

UNE-ISO/IEC 19770-1:2008 *Tecnología de la Información. Gestión de activos de software (SAM). Parte 1: Procesos.*

Hace referencia a la primera parte de la norma 19770, en la que se determinan los procesos que deberían componer un sistema de gestión de activos de software. Estos procesos se denominan Software Asset Managament/ Gestión de activos Software - SAM. **[59]**

ISO/IEC 29110:2011 *Ingeniería Software – Perfiles de ciclo de vida para Entidades Muy Pequeñas*. **[60]**

Indica las características y los requisitos de las VSE (Very Small Entity/Entidades Muy Pequeñas) y proporciona un conjunto de normas y guías, en las se incluye un conjunto de procesos y modelos para poder adoptar la norma. También están incluidos los términos de negocio comunes en la serie ISO/IEC 29110.

La ISO/IEC TR 29110-1:2011 es aplicable a VSEs, pues los procesos de ciclo de vida descritos en ISO/IEC 29110 no excluyen su utilización en entidades más grandes que un VSE.

ISO/IEC 25000:2014 Sistemas e *Ingeniería de Software - Requisitos de Calidad y Evaluación de Productos de Software (SQuaRE) - Guía de SquaRE.*

La serie de la ISO/IEC 25000 cuenta con cinco ramas:

ISO/IEC 2500n – División para la gestión de la calidad.
ISO/IEC 2501n – División para el modelo de calidad.
ISO/IEC 2502n – División para la medición de la calidad.
ISO/IEC 2503n – División para los requisitos de la calidad.
ISO/IEC 2504n – División para la evaluación de la calidad.

Dentro de la división ISO/IEC 2500n, encontramos la ISO 25000:2005, que define el modelo de arquitectura SQuaRE, las partes implicadas y la terminología común. **[61]** **[62]** Estos aspectos, junto con el establecimiento de la relación entre los documentos, facilita a los usuarios la comprensión de la norma de acuerdo con su propósito de uso. **[63]**

ISO/IEC/IEEE 29119:2013 *Pruebas de Software*. **[64]**

La norma pretende ser un referente internacional en materia de pruebas software. Está dividida en las siguientes partes:

ISO/IEC/IEEE 29119-1:2013: Parte 1: Conceptos y definiciones.
ISO/IEC/IEEE 29119-2:2013: Parte 2: Procesos de prueba.
ISO/IEC/IEEE 29119-2:2013: Parte 3: Documentación de las pruebas.

Contempla todas las etapas del ciclo de vida software y toma como referencia las principales normas relacionadas con la realización de pruebas software, con los modelos de ciclos de vida y de procesos:

- BSI (British Standards Institution – Instituto Británico de Normalización): BS 7925-1, Pruebas de Software: Parte 1-Vocabulario y BS 7925-2, Pruebas de Software: Parte 2-Pruebas de Componentes Software.

- IEEE: IEEE Std. 829, Documentación de Pruebas Software e IEEE Std 1008, Pruebas Software Unitarias; IEEE Std 1012-1998, Verificación y Validación Software y IEEE Std 1028-1997, Revisiones Software.

- ISO/IEC: ISO/IEC 12207, Procesos de Ciclo de Vida de Software; ISO/IEC 15289 Productos de Información del Ciclo de Vida de Procesos Software y de Sistemas y ISO/IEC TR 19759, Guía de Conocimiento de Ingeniería Software.

Capítulo 3
Auditoría y Control según la norma UNE-ISO/IEC 38500:2013

Se presenta el planteamiento del problema y la solución propuesta.

En el apartado *3.1 Planteamiento del problema*, se describe el problema y los riesgos vinculados al uso de la tecnología de la información.

El apartado *3.2 Propuesta de la solución*, describe cada una de las propuestas que dan solución al correspondiente problema planteado.

El último apartado, 3.*3 Auditoría y control según la norma UNE-ISO/38500: 2013 – cuestionario de autoevaluación*, se describen los requisitos del cuestionario de autoevaluación, que implementa la solución planteada en el apartado 3.2.

3.1 Planteamiento del problema

Se ha definido en puntos anteriores el papel de las tecnologías de la información en la empresa y su función estratégica. Para completar esta visión, planteemos la siguiente cuestión: en una organización, si el departamento de marketing no está operativo durante una semana, ¿qué ocurre?, ¿puede la empresa seguir funcionando con normalidad? Y si ahora, en lugar de ser el departamento de marketing son las tecnologías de la información las que no funcionan u operan correctamente, ¿podría la empresa seguir funcionando con normalidad?, ¿tendría el mismo impacto que el primer supuesto?

Otro problema vinculado con la T.I es que suelen representar un porcentaje elevado del total del presupuesto o de los costes de una organización y, con bastante frecuencia, no se produce un retorno de la inversión. El origen de estos fracasos suele venir determinado por dar mayor importancia a la tecnología, a las finanzas y a aspectos de la planificación de las actividades de T.I que al contexto global del uso de la tecnología de la información en el negocio. Entonces, ¿cómo se puede obtener valor de las inversiones T.I? Hace falta una normativa que regule su uso y facilite su gestión.

Por tanto, si la T.I absorbe cada vez más tiempo y capital y su uso afecta a la capacidad estratégica de la empresa, no debería ser el departamento informático o el de sistemas el que decidiera sobre estas cuestiones, habría que delegar a la alta dirección la capacidad de decisión de todas aquellas decisiones relacionadas o vinculadas con las T.I.

Habrá además que evaluar, monitorizar y establecer las pautas para dirigir las actividades T.I, con el fin de garantizar la consecución de los metas de negocio, para ello será necesario determinar el grado de cumplimiento y desarrollo de los procesos respecto a los modelos internacionales. Se debe también prestar atención a la seguridad y al control de la T.I, cuyo objetivo es gestionar los riesgos relacionados con la tecnología de la información y minimizar su impacto.

3.2 Propuesta de la solución

3.2.1 La norma, UNE- ISO/IEC 38500:2013

Esta norma va proporcionar a los directores el marco necesario para garantizar que el uso de la información dentro de sus organizaciones es práctico, eficiente y adecuado.

Se resumen a continuación los aspectos principales de la norma, extraídos de la publicación de AENOR.

3.2.1.1 Alcance, aplicación y objetivos

La norma fue diseñada para poder ser utilizada en cualquier organización, independientemente de su tamaño o sector. **[54]**

Promueve su objetivo de gobernanza de las tecnologías de la información de las siguientes formas **[16]**:

- Mediante el asesoramiento a los directores en las actividades de gobierno T.I.
- Garantizar con la implantación de la norma que las tareas de gobierno se están llevando a cabo de forma correcta, consiguiendo así el apoyo y la confianza de las partes interesadas.
- Proporciona las bases para poder llevar a cabo una evaluación objetiva de las T.I.

Otro objetivo, probablemente el más deducible por el propio contexto y el alcance de la propia norma, es "el gobierno de los procesos y de las decisiones relacionadas con la información que sean utilizadas en la organización". **[54]**

La conformidad y el rendimiento, son dos de los beneficios principales que toda organización puede obtener del seguimiento de la norma **[16]**:

- Conformidad. Los directores que ejerzan un adecuado gobierno sobre las T.I podrán abordar de manera más adecuada los riesgos asociados con su uso y cumplir con los requisitos establecidos.
- Gestión de costes eficiente. Los directores no tienen sólo la responsabilidad de cumplir con la normativa legal tienen también que generar beneficios, lo que en ocasiones implica asumir riesgos económicos pues el retorno de inversión no está siempre asegurado. La norma, al igual que para la conformidad, identifica una serie de formas en las que puede contribuir al desempeño de la organización.

3.2.1.2 La norma como marco de referencia

Esta parte de la norma es la más importante del estándar y es el concepto principal para el gobierno T.I, en la que se identifican seis principios de buen gobierno y tres tareas principales, bajo un modelo de gobierno, de las que son responsables los directores. **[16]**

Principios

Cada principio establece una serie de indicaciones para guiar la toma de decisiones, pero no describe las pautas para implantarlos, pues van a depender de cada organización en la que se vayan a aplicar.

1. **Responsabilidad**. Establece que los responsables de la tecnología de la información dentro de una empresa deben tener la autoridad suficiente para llevar a cabo todas las acciones y medidas necesarias para desarrollar las actividades de las que son responsables.

2. **Estrategia.** La estrategia de negocio de una organización debe tener en consideración la capacidad presente y futura; Mientras que la estrategia T.I debería reflejar los requisitos de la estrategia de negocio, es lo que suele denominar alineación de negocio con las T.I.

3. **Adquisición.** Este principio establece que cualquier inversión que se vaya a realizar debe quedar lo suficientemente clara, hay que evaluar previamente la relación entre el coste y el beneficio, y comprender los riesgos. Este análisis debe hacerse para determinar su impacto actual y futuro.

4. **Desempeño**. Las Tecnologías de Información deben ser aptas para el propósito para el que han sido diseñadas o utilizadas.

5. **Cumplimiento**. Debido a la dependencia de la organización respecto a las T.I, debe garantizarse que cumple con todos los requisitos regulatorios y con la normativa correspondiente.

6. **Conducta Humana**. Las T.I también dependen de los recursos humanos, por lo que es necesario fijar las políticas, prácticas y decisiones T.I relacionadas con el comportamiento humano.

Modelo de gobierno

La norma UNE- ISO/IEC 38500 sugiere el siguiente modelo de gobierno T.I (Figura 10):

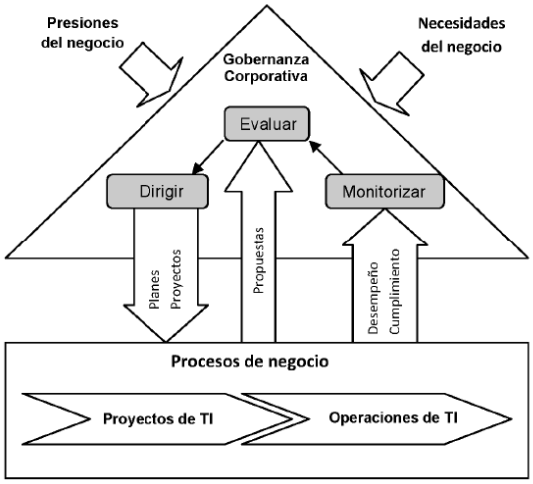

Figura 10. Modelo de gobierno corporativo T.I de la norma ISO 38500.

Propone que los directores dirijan las Tecnologías de la Información mediante tres acciones principales:

Evaluar. Los directores deben evaluar el uso presente y futuro de las T.I, incluyendo los planes de implementación, estrategias, acuerdos de servicios, etc. Deben tener en cuenta todos los factores que influyen en el negocio, como pueden ser una nueva tendencia económica, tecnológica o incluso cambios normativos. Las evaluaciones deben realizarse de forma regular y es importante que sean informados de su resultado para, en base a los mismos, tomar las decisiones de negocio adecuadas.

Dirigir. Es tarea de la Junta o del consejo de dirección asignar las responsabilidades para la ejecución y el cumplimiento de los planes y las políticas T.I. Para que las decisiones sean correctas, debe garantizarse que la Dirección cuenta con la información correcta y actualizada de las operaciones y proyectos T.I. Esta información también les permitirá conocer si estas se están ejecutando según lo planificado.

Del modelo, probablemente sea la acción más importante, ya que se definen las condiciones y las operativas de negocio, que si resultan adecuadas garantizarán la ejecución correcta de los proyectos y los procesos, y en la cual se han contemplado todos los posibles factores o riesgos que pueden afectar al éxito de los mismos.

Monitorizar. Los sistemas de monitorización permitirán obtener información sobre lo que está pasando y alertará sobre cualquier incumplimiento del servicio, de las normas, etc. La auditoría interna es una parte de monitorización tan importante como lo son informes de gestión de cuentas y de rendimiento.

3.2.1.3 Adopción de la norma UNE- ISO/IEC 38500:2013

En la actualidad existen varias herramientas que soportan la gestión T.I pero no hay un número muy elevado que permitan la implantación del gobierno T.I en una organización. Podemos ver en la siguiente tabla (Tabla 1), a modo de esquema, los diferentes estándares que apoyan las áreas relacionadas con las Tecnologías de la Información **[65]**:

	ESTÁNDAR INTERNACIONAL	ESTÁNDAR NACIONAL	MARCO DE REFENCIA
Gobierno de las T.I.	**ISO 38500**	**AS 8015** **COSO [b]**	**COBIT**
Planificación T.I.		PSI-Métrica 3	
Valor de las T.I.			Val IT
Gestión Servicios T.I.	ISO/IEC 20000	BS 15000	COBIT ITIL MOF
Gestión de Proyectos.		UNE 15781	PMBOK PRINCE2 APMs IPMA
Desarrollo Software.	ISO 12207 ISO 15504	Ticket Métrica 3	CMMI Bootstrap
Gestión de Riesgos.		AS/NZS 4360 COSO Magerit UNE 71504	
Gestión de Seguridad.	ISO 27000 ISO 13335 ISO 13569 ISO 17799 ISO 15408	NIST-800 series BS 7799-2 GAO´s FISCAM German BSI	ASCI-33 COBIT ISF ENV12924 SEI´s OCTAVE SEI´s SW-CMM BPM
Gestión de Continuidad.	ISO /IEC 25999	PAS-56 AS/NZS 4360 HB 221-2004 BS25999	
Gestión de la Calidad.	ISO 9001	EFQM BNQP SixSigma	
Auditoría.	ISO 19011		COBIT

Tabla 1. Herramientas para la implementación del Gobierno de las T.I. **[65]**

Se puede utilizar también como guía, para la implantación de gobierno T.I, el estudio realizado por el ITIG, en el que se detallan los productos ITIG que lo apoyan y que permiten además la adopción de la norma UNE- ISO/IEC 38500. En el estudio se señala por cada producto qué principio de la norma y qué acción del modelo soportan **[66]**. (Ver Figura 11).

	Principios UNE-ISO/IEC 38500						Tareas		
Productos ITIG	Responsabilidad	Estrategia	Adquisición	Desempeño	Cumplimiento	Conducta humana	Evaluar	Dirigir	Monitorizar
Informe del Consejo sobre Gobierno T.I, 2ª Edición. (Unlocking Value: An Executive Primer on the Critical Role of IT Governance.)	x	x				x	x	x	x
Generando Valor: Un manual básico del ejecutivo sobre el papel crítico de Gobierno de T.I. (Unlocking Value: An Executive Primer on the Critical Role of IT Governance.)	x	x				x	x	x	x
COBIT.	x	x	x	x	x	x	x	x	x
Val IT.	x	x	x	x	x	x	x	x	x
Guía de Implementación de Gobierno T.I: Usando COBIT y Val IT, 2ª Edición (IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition.)							x	x	x
Guía de Aseguramiento T.I: Usando COBIT. (IT Assurance Guide: Using COBIT.)				x	x		x		x
Guía rápida de COBIT, 2ª Edición (COBIT Quickstart, 2nd Edition.)							x	x	
Valor de Empresa: Gobernanza de las inversiones T.I, Introducción a la Gestión del Valor. (Enterprise Value: Governance of IT Investments, Getting Started With Value Management.)							x		
COBIT Seguridad de Referencia, 2ª Edición. (COBIT® Security Baseline™, 2nd Edition.)	x						x	x	

Figura 11. Relación de productos ITGI y UNE-ISO/IEC 38500. **[66]**

Como la norma UNE- ISO/IEC 38500 establece las pautas o tareas a realizar, pero no define cómo o quién llevarlas a cabo, hace falta un marco que sirva de apoyo y guía para aquellas empresas que quieran implantarla. Utilizando como fuente las tablas anteriores, podemos concluir que la elección de COBIT como marco referente será una de las mejores opciones.

COBIT cuenta con varias versiones, de ellas, para la realización del proyecto se ha elegido la quinta versión -COBIT 5- que a fecha actual es la última versión publicada por ISACA. El motivo de la elección es en primer lugar debido a la naturaleza del proyecto, en el que se manifiesta y reitera el uso de las T.I como elemento estratégico y generador de valor en la empresa: si se trasladara el proyecto al entorno real de negocio, para una empresa, la evaluación respecto a la última versión del marco podría suponer una ventaja competitiva respecto al resto de organizaciones. Si existe una nueva versión ya estable de una tecnología, procedimiento, estándar… por qué utilizar una versión anterior, hay que posicionarse en el mercado e innovar. La segunda justificación de la elección del marco viene dada porque este nos proporciona un mayor abanico de posibilidades a la hora de

definir los criterios para realizar la evaluación el nivel de madurez de la empresa, que otras versiones, como se detallará en el siguiente punto (3.2.2).

3.2.1.3.1 Adopción del estándar mediante COBIT 5

¿De qué forma contribuye entonces COBIT 5 a la adopción del estándar UNE-ISO/IEC 38500?

Se describen a continuación, en base a la información que el propio marco facilita, por cada uno de los principios de la norma ISO qué procesos de COBIT lo soportan.

Principio 1 – Responsabilidad.

- Entre los catalizadores que define COBIT 5 para el gobierno T.I, destacan el de *proceso* y el de *estructuras organizativas*, en los que se describen los roles y responsabilidades que van a intervenir. Se incluyen también una serie de ejemplos que pueden ser orientativos para la Dirección.
- Del conjunto de procesos, EDM05 describe la función de la Dirección en las tareas de supervisar y evaluar el gobierno T.I.

Principio 2 – Estrategia.

- El proceso EDM02 hace referencia a la gestión de la inversión T.I. y al modo en el que los casos de negocio deben apoyar los objetivos empresariales.
- El dominio APO incluye los procesos relacionados con la gestión y planificación de recursos T.I. Incluye también una serie de ejemplos que ayudan a la alineación de las metas corporativas y los procesos T.I.

Principio 3 – Adquisición.

- El dominio EDM analiza los requerimientos de gobierno T.I para garantizar que se cumple la entrega de beneficios, la optimización de costes de los recursos y se tiene identificado el impacto de los riesgos T.I en el valor de la empresa.
- El dominio APO se encarga de planificar, alinear y organizar las actividades relacionadas con la adquisición.
- El dominio BAI define los procesos indispensables para llevar a cabo la implementación T.I.
- El dominio MEA junto con el proceso EDM05 indican cómo pueden realizarse las tareas de evaluación y supervisión de la adquisición, así como las medidas de control interno para asegurar que su gestión es correcta.

Principio 4 – Rendimiento.

- Los procesos APO02 y APO09 hacen referencia respectivamente a la definición de objetivos y al establecimiento de los servicios.
- El proceso MEA01 se encarga de supervisar y determinar si el rendimiento de los procesos T.I es el adecuado y conforme a los requisitos establecidos.

Principio 5 – Conformidad.

- El proceso APO02 se encarga de alinear la estrategia empresarial T.I con los objetivos de negocio.
- El proceso MEA02 realiza una evaluación de los controles para detectar posibles deficiencias en los mismos y poder elaborar mecanismos de mejora.
- El proceso MEA03 permite garantizar que se identifican y cumplen los requisitos de todos aquellos procesos relacionados con las T.I.

Principio 6 – Comportamiento humano.

- El proceso APO07 tiene como fin mejorar las habilidades y capacidades de los usuarios con el objetivo de conseguir de una manera más eficaz y eficiente los objetivos de la entidad.
- El proceso BAI02 es el encargado de la gestión de requisitos.
- Los procesos BAI05 y BAI08 hacen referencia a la formación de los usuarios, necesaria para que puedan responder ante cambios y realizar sus tareas de forma correcta.

En relación al modelo propuesto por la UNE-ISO/IEC 38500, las tareas de evaluar, dirigir y monitorizar quedarían cubiertas con el dominio EDM de COBIT 5, en el que cada uno de sus procesos tiene definidas las actividades de evaluar, orientar y supervisar.

Partiendo de las indicaciones anteriores se ha elaborado la siguiente tabla (Tabla 2), en la que se define el mapeo correspondiente entre cada uno de los principios de la norma UNE-ISO/IEC 38500 y los procesos de COBIT 5 que los apoyan. Comentar que, en nuestra propuesta, un mismo proceso puede respaldar a más de un principio y también se da la casuística de procesos que no apoyan a ningún principio.

P	Proceso Principal
S	Proceso Secundario
	Proceso No incluido

	Principios UNE-ISO/IEC 38500					
	Responsabilidad	Estrategia	Adquisición	Desempeño	Cumplimiento	Conducta humana
	1	2	3	4	5	6
Procesos COBIT 5						

EDM								
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	P	S		P		
	EDM02	Asegurar la Entrega de Beneficios.	P	S		P	S	
	EDM03	Asegurar la Optimización del Riesgo.	P	S	S	P		S
	EDM04	Asegurar la Optimización de los Recursos.	P			P		
	EDM05	Asegurar la Transparencia hacia las partes interesadas.	P					
AP0								
Alinear, Planificar y Organizar.	APO01	Gestionar el Marco de Gestión de TI.		P	S			P
	APO02	Gestionar la Estrategia.		P		P	P	
	APO03	Gestionar la Arquitectura Empresarial.		P				
	APO04	Gestionar la Innovación.		P				
	APO05	Gestionar el portafolio.		S	S	S	S	
	APO06	Gestionar el Presupuesto y los Costes.		P	P			
	APO07	Gestionar los Recursos Humanos.		P				P
	APO08	Gestionar las Relaciones.						
	APO09	Gestionar los Acuerdos de Servicio..				P		
	APO10	Gestionar los Proveedores.			P			
	APO11	Gestionar la Calidad.		P	P			S
	APO12	Gestionar el Riesgo.		P	P			
	APO13	Gestionar la Seguridad.						
BAI								
Construcción, Adquisición e Implementación.	BAI01	Gestionar los Programas y Proyectos.		P	P			
	BAI02	Gestionar la Definición de Requisitos			P			P
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.			P			P
	BAI04	Gestionar la Disponibilidad y la Capacidad.						
	BAI05	Gestionar la introducción de Cambios Organizativos.			S			S
	BAI06	Gestionar los Cambios.			P			
	BAI07	Gestionar la Aceptación del Cambio y de la Transición.			P			
	BAI08	Gestionar el Conocimiento.			P			P
	BAI09	Gestionar los Activos.						
	BAI10	Gestionar la Configuración.						
DSS								
Entregar, dar Servicio y Soporte.	DSS01	Gestionar las Operaciones.						
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio.						

	DSS03	Gestionar los Problemas.						
	DSS04	Gestionar la Continuidad.						
	DSS05	Gestionar los Servicios de Seguridad.						
	DSS06	Gestionar los Controles de los Procesos del Negocio.		S				S
MEA								
Supervisión, Evaluación y Verificación.	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.			P	P		
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	P		P	P	P	P
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.					P	

Tabla 2. Mapeo Principios de la norma UNE-ISO/IEC 38500 - Procesos de COBIT 5.

Para facilitar la interpretación y lectura de la tabla anterior, se muestra a continuación su tabla equivalente organizada en base a cada principio de la norma UNE-ISO/IEC 38500:

Responsabilidad			
	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	P
	EDM02	Asegurar la Entrega de Beneficios.	P
	EDM03	Asegurar la Optimización del Riesgo.	P
	EDM04	Asegurar la Optimización de los Recursos.	P
	EDM05	Asegurar la Transparencia hacia las partes interesadas.	P
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	P
Estrategia			
	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	S
	EDM02	Asegurar la Entrega de Beneficios.	S
	EDM03	Asegurar la Optimización del Riesgo.	S
	APO01	Gestionar el Marco de Gestión de TI.	P
	APO02	Gestionar la Estrategia.	P
	APO03	Gestionar la Arquitectura Empresarial.	P
	APO04	Gestionar la Innovación.	P
	APO05	Gestionar el portafolio.	S

	APO06	Gestionar el Presupuesto y los Costes.	P
	APO07	Gestionar los Recursos Humanos.	P
	APO11	Gestionar la Calidad.	P
	APO12	Gestionar el Riesgo.	P
	BAI01	Gestionar los Programas y Proyectos.	P
	DSS06	Gestionar los Controles de los Procesos del Negocio.	S
	EDM03	Asegurar la Optimización del Riesgo.	S
	APO01	Gestionar el Marco de Gestión de TI.	S
	APO05	Gestionar el portafolio.	S
	APO06	Gestionar el Presupuesto y los Costes.	P
	APO10	Gestionar los Proveedores.	P
	APO11	Gestionar la Calidad.	P
	APO12	Gestionar el Riesgo.	P
	BAI01	Gestionar los Programas y Proyectos.	P
	BAI02	Gestionar la Definición de Requisitos.	P
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.	P
	BAI05	Gestionar la introducción de Cambios Organizativos.	S
	BAI06	Gestionar los Cambios.	P
	BAI07	Gestionar la Aceptación del Cambio y de la Transición.	P
	BAI08	Gestionar el Conocimiento.	P
	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	P
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	P
Adquisición			
	EDM03	Asegurar la Optimización del Riesgo.	S
	APO01	Gestionar el Marco de Gestión de TI.	S
	APO05	Gestionar el portafolio.	S
	APO06	Gestionar el Presupuesto y los Costes.	P
	APO10	Gestionar los Proveedores.	P
	APO11	Gestionar la Calidad.	P
	APO12	Gestionar el Riesgo.	P
	BAI01	Gestionar los Programas y Proyectos.	P
	BAI02	Gestionar la Definición de Requisitos.	P
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.	P

	BAI05	Gestionar la introducción de Cambios Organizativos.	S
	BAI06	Gestionar los Cambios.	P
	BAI07	Gestionar la Aceptación del Cambio y de la Transición.	P
	BAI08	Gestionar el Conocimiento.	P
	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	P
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	P
Desempeño			
	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	P
	EDM02	Asegurar la Entrega de Beneficios.	P
	EDM03	Asegurar la Optimización del Riesgo.	P
	EDM04	Asegurar la Optimización de los Recursos.	P
	APO02	Gestionar la Estrategia.	P
	APO05	Gestionar el portafolio.	S
	APO09	Gestionar los Acuerdos de Servicio.	P
	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	P
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	P
Cumplimiento			
	EDM02	Asegurar la Entrega de Beneficios.	S
	APO02	Gestionar la Estrategia.	P
	APO05	Gestionar el portafolio.	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	P
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	P
Conducta humana			
	EDM03	Asegurar la Optimización del Riesgo.	S
	APO01	Gestionar el Marco de Gestión de TI.	P
	APO07	Gestionar los Recursos Humanos.	P
	APO11	Gestionar la Calidad.	S
	BAI02	Gestionar la Definición de Requisitos.	P
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.	P
	BAI05	Gestionar la introducción de Cambios Organizativos.	S
	BAI08	Gestionar el Conocimiento.	P

	DSS06	Gestionar los Controles de los Procesos del Negocio.	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	P

Tabla 3. Mapeo Principios de la norma UNE-ISO/IEC 38500 - Procesos COBIT 5, en base a los principios.

3.2.2 Evaluar la organización

Definida ya la relación entre COBIT 5 y la norma UNE-ISO/IEC 38500, llegamos a uno de los puntos principales del proyecto, el permitir evaluar una organización en base a la norma UNE-ISO/IEC 38500 y obtener el grado de cumplimiento. ¿Cómo plantearlo?

Vamos a hacerlo a partir de la evaluación de cada uno de los procesos de COBIT que apoyan a los principios del estándar (ver Tabla 3 a modo de recordatorio) y en base a sus resultados, mediante la lógica correspondiente, obtener el resultado de cada principio.

La versión de COBIT 4 cuenta con un procedimiento propio para determinar el nivel de madurez de cada uno de los procesos, pero en la versión COBIT 5 ha sido sustituido y lo que se evalúa es su nivel de capacidad (mencionar también que los procesos entre ambas versiones difieren, aunque en algunos casos se han establecido equivalencias; por este motivo no vamos a emplear el modelo de evaluación de COBIT 4 para medir los procesos de COBIT 5). Por tanto, vamos a utilizar otro modelo o herramienta que nos permita determinar el nivel de madurez de los procesos y a aprovechar el modelo de COBIT 5 para obtener la capacidad de los procesos, es decir, medir su desempeño.

Es decir, por cada proceso se van a realizar dos tipos de evaluación, una para obtener su nivel de capacidad y otra para determinar su nivel de madurez:

- La capacidad se obtendrá mediante el modelo propio de COBIT 5, que está basado en la norma ISO/IEC 15504 de *Ingeniería de Software - Evaluación de Procesos*, y que va a permitir obtener el grado de cumplimiento de cada proceso. En base a esta norma, y una vez evaluados todos los procesos, resultará fácil poder calcular el nivel de madurez de una organización. Basta con definir qué procesos compondrán cada nivel de madurez y verificar si alcanzan el nivel de capacidad definido en cada nivel.
- Para obtener el nivel de madurez se va utilizar el Modelo de Madurez de Proceso y de Empresa (PEMM).

Esta propuesta nos va a permitir, por tanto:

- Obtener el nivel de madurez de cada principio de la norma UNE-ISO/IEC 38500 en base al nivel de madurez de los procesos que lo componen.
- Determinar el alcance de la organización, mediante la puntuación obtenida en la evaluación por niveles de madurez de la organización. En base a esa puntuación la empresa podrá determinar el conjunto de procesos que hay que completar o llevar a cabo para obtener el nivel de madurez objetivo.

- La evaluación por niveles de capacidad permitirá a la organización conocer los procesos específicos a mejorar, a partir de la puntuación a nivel de procesos que se realiza. Resultará útil para determinar cuáles son los procesos a completar para alcanzar el nivel de madurez deseado de cada principio de la norma UNE-ISO/IEC 38500.

En los siguientes puntos se detallan las características de evaluaciones mencionadas.

3.2.2.1 Evaluación del nivel de capacidad de los procesos

El marco COBIT 5 define seis niveles de capacidad para cada proceso, comprendidos del cero al cinco **[67]**:

Nivel 0, incompleto. En este nivel el proceso no cumple ninguno, o un número muy bajo, de los objetivos para los que ha sido diseñado.

Nivel 1, ejecutado. Si el proceso satisface todos sus requisitos de diseño.

Nivel 2, gestionado. En este nivel se supervisa y planifica el proceso y se asegura la estabilidad de los resultados.

Nivel 3, establecido. Además de estar operativo el proceso y de que su salida sea correcta, estos resultados obtenidos son los definidos para el proceso.

Nivel 4, predecible. Los resultados están dentro del rango de aceptación definido.

Nivel 5, optimizado. En este nivel se llevan a cabo tareas mejora continua del proceso.

A continuación, para cada objetivo definido por nivel de capacidad y proceso, se determina su grado de alcance:

No Alcanzado (NA). Si apenas hay evidencia del logro del objetivo. En términos de porcentaje se indica que el logro está entre el cero y el quince por ciento.

Parcialmente Alcanzado (PA). Si se cumplen menos de la mitad de los objetivos del proceso. Es decir, un porcentaje de logro comprendido entre el dieciséis y el cincuenta por ciento.

Ampliamente Alcanzado (AA). Cuando, salvo por algunas deficiencias, se cumplen casi la totalidad de los objetivos del proceso evaluado. Lo que equivaldría a un porcentaje entre el cincuenta y uno y el ochenta y cinco por ciento de logro.

Completamente Alcanzado (CA). Se logran de manera completa los objetivos y no hay evidencias de debilidades. El porcentaje de logro está entre el ochenta y seis y el cien por cien.

El procedimiento de cálculo es el siguiente: para obtener un determinado nivel de capacidad debe cumplirse que el nivel inferior esté calificado como CA (Completamente Alcanzado), y, además, que el nivel evaluado sea CA (Completamente Alcanzado) o AA (Ampliamente Alcanzado). Por ejemplo, un nivel 3 de capacidad de proceso (establecido) requiere la consecución completa de los objetivos del nivel 2 de madurez de los procesos (proceso gestionado).

Otras consideraciones, de carácter propio, a tener en cuenta para calcular el nivel de capacidad de un proceso:

- Si un proceso no está implementado, su nivel de capacidad será cero.
- Si se cumple alguno de los atributos de nivel 1, el nivel de capacidad será uno.
- Se considera que un nivel es AA o CA si la mitad más una de las cuestiones que componen dicho valor tienen ese valor.

3.2.2.2 Evaluación del nivel de madurez de la organización

Para la evaluación del nivel de madurez de la organización se define también un modelo de seis niveles **[68]**:

Nivel 0, inmadura. No hay procesos definidos, es un nivel inicial donde la organización es inmadura y sus procesos deben ser mejorados incluso iniciados.

Nivel 1, básica. La organización desarrolla y logra los objetivos de los procesos. En este nivel la organización alcanza el propósito de los procesos.

Nivel 2, gestionada. Los procesos se planifican, ejecutan, miden y controlan. Una organización que tenga una madurez de nivel dos cumple con los siguientes requisitos:

- Establece planes y procedimientos para realizar los procesos.
- Asigna las responsabilidades a cada proceso.
- Asigna los recursos y la información adecuada.
- Realiza un seguimiento respecto a los planes y procedimientos.
- Toma acciones para tratar las desviaciones.
- Identifica los requisitos para la gestión de los productos de trabajo de los procesos.
- Toma acciones para asegurar que estos requisitos se cumplen.
- Asienta las bases metodológicas para poder medir la mejora real de los procesos.

Nivel 3, establecido. En este nivel, los procesos de la organización se adaptan a partir del conjunto de procesos estándar de la organización. Una organización de nivel tres:

- Establece descripciones del proceso estándar.
- Asegura que los procesos se adaptan a partir del conjunto de procesos estándar.
- Recoge y analiza los datos para comprender la efectividad del proceso adaptado.

- Utiliza los datos recogidos para mejorar el conjunto de procesos estándar y los procesos adaptados.

Nivel 4, predecible. La organización se centra en que los resultados de los procesos sean los esperados. Una organización de nivel cuatro lleva a cabo las siguientes actividades:

- Establece objetivos cuantitativos de rendimiento de los procesos alineados con los objetivos de negocio.
- Selecciona procesos para el análisis de rendimiento.
- Se recogen, almacenan y analizan datos sobre el rendimiento de los procesos seleccionados.
- Identifica las causas de variación en el rendimiento de los procesos y lleva a cabo las acciones correctivas necesarias.
- Establece un rendimiento de los procesos estable, capaz y predecible dentro de los límites de control definidos.

Nivel 5, optimizando. La organización mejora de forma continua los procesos basándose en el análisis de las causas que afectan a su rendimiento. Una organización de nivel cinco:

- Identifica las causas comunes de variación del rendimiento de los procesos, basándose en los resultados de los análisis, e identifica las mejoras.
- Identifica innovaciones para mejorar el rendimiento de los procesos y el éxito del negocio.
- Identifica oportunidades de mejora con el control de riesgos asociados.
- Recoge y analiza datos para seleccionar mejoras para la organización, basadas en el impacto en el rendimiento de los procesos y en el éxito del negocio.
- Utiliza las mejoras, controla el rendimiento de los procesos mejorados, y compara los resultados con los valores esperados.

En base a este modelo se van a clasificar los procesos de COBIT, que apoyen la norma UNE-ISO/IEC 38500, por nivel de madurez de manera que cada nivel va a comprender aquellos procesos que permitan dar soporte a su comportamiento. Teniendo en cuenta estas premisas se ha elaborado la siguiente clasificación (Tabla 4):

Nivel de madurez de la organización	**Procesos**
Nivel 0, Inmadura.	No existen procesos definidos en este nivel.
Nivel 1, Básica.	BAI02. Gestionar la Definición de Requisitos.
	BAI03. Gestionar la Identificación y la Construcción de Soluciones.
	BAI07. Gestionar la Aceptación del Cambio y de la Transición.
Nivel 2, Gestionada.	APO01. Gestionar el Marco de Gestión de T.I.
	APO02. Gestionar la Estrategia.
	APO09. Gestionar los Acuerdos de Servicio.

	APO10. Gestionar los Proveedores.
	BAI01. Gestionar los Programas y Proyectos.
	BAI06. Gestionar los Cambios.
	DSS06. Gestionar los Controles de los Procesos del Negocio.
Nivel 3, Establecido.	APO03. Gestionar la Arquitectura Empresarial.
	APO05. Gestionar el portafolio.
	APO07. Gestionar los Recursos Humanos.
	BAI05. Gestionar la introducción de Cambios Organizativos.
	BAI08. Gestionar el Conocimiento.
Nivel 4, Predecible.	APO06. Gestionar el Presupuesto y los Costes.
	APO12. Gestionar el Riesgo.
	MEA01. Supervisar, Evaluar y Valorar Rendimiento y Conformidad.
	MEA03. Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.
Nivel 5, Optimizando.	EDM01. Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.
	EDM02. Asegurar la Entrega de Beneficios.
	EDM03. Asegurar la Optimización del Riesgo.
	EDM04. Asegurar la Optimización de los Recursos.
	APO04. Gestionar la Innovación.
	APO11. Gestionar la Calidad.
	MEA02. Supervisar, Evaluar y Valorar el Sistema de Control Interno.

Tabla 4. Procesos definidos por nivel de madurez.

Una vez evaluados los procesos por nivel de capacidad y utilizando el modelo propuesto por la ISO/IEC TR 15504-7:2008, se obtendrá el nivel de madurez de la organización conforme a las siguientes reglas de derivación:

Nivel de madurez de la organización	**Descripción**
Nivel 0, Inmadura.	La organización no tiene una implementación efectiva de los procesos.
Nivel 1, Básica.	Los procesos objeto de evaluación, incluidos en este nivel, alcanzan el nivel de capacidad 1, es decir, existen productos resultantes para los mismos y el proceso se puede identificar.
Nivel 2, Gestionada.	Los procesos del nivel de madurez 2 tienen nivel de capacidad 2 o superior.
Nivel 3, Establecido.	Los procesos de los niveles de madurez 2 y 3 tienen nivel de capacidad 3 o superior.
Nivel 4, Predecible.	Uno o más procesos tienen nivel de capacidad 4 o superior.
Nivel 5, Optimizando.	Uno o más procesos tienen nivel de capacidad 5.

Figura 12. Reglas de derivación para los niveles de madurez. [ISO/IEC TR 15504-7:2008] **[68]**

Para que una organización alcance un determinado nivel de madurez debe satisfacer también las condiciones de los niveles inferiores. Es un proceso gradual, por ejemplo, para obtener el nivel de madurez 4 debe cumplir también los requisitos de los niveles 1, 2 y 3.

3.2.2.3 Evaluación del nivel de madurez de los procesos

Tras la búsqueda detallada para encontrar un modelo alternativo al propuesto por COBIT 4, que nos permitiera realizar la evaluación de los procesos para obtener su nivel de madurez, finalmente se optó por un modelo cuyo enfoque se ajustaba a nuestro planteamiento. Se trata del Modelo de Madurez de Procesos y Empresa (PEMM) desarrollado por Michael Hammer.

M. Hammer define cinco características clave para garantizar el buen funcionamiento de un proceso **[69]:**

- Sus especificaciones de diseño deben ser lo más exactas y completas posible; de otro modo, la gente que lo ejecuta no sabrá qué hacer o cuándo.
- Las personas que desarrollen o ejecuten el proceso deben poseer las habilidades y conocimientos apropiados; de lo contrario, no podrán implementar el diseño.
- Debe haber un responsable, que será quien garantice la consecución de los resultados del proceso; de otra manera, el proceso se perderá dentro del sistema.
- La empresa debe alinear su infraestructura –como las tecnologías de información y los sistemas de recursos humanos– para apoyar el proceso; sino, debilitarán su desempeño.
- Finalmente, la empresa debe evaluar el desempeño del proceso para que los resultados obtenidos sean los correctos.

A estas características se las denomina "facilitadores de proceso". Por cada facilitador, el modelo PEMM propone una serie de afirmaciones y cuatro grados de alcance por afirmación: P1, P2, P3, P4. Para cada afirmación hay que determinar qué nivel de alcance logra.

Para que la nomenclatura del grado de alcance esté unificada con las otras evaluaciones propuestas en el proyecto vamos a renombrarla, de manera que:

- P1 da lugar a NA (No Alcanzado).
- P2 se renombra a PA (Parcialmente Alcanzado).
- P3 a AA (Ampliamente Alcanzado).
- Y P4 a CA (Completamente Alcanzado).

Donde:

No Alcanzado (NA), es el grado de alcance correspondiente si la afirmación evaluada no es cierta en gran medida. (Entre el uno y el quince por ciento.)

Parcialmente Alcanzado (PA), es el alcance cuando la afirmación es cierta en cierto grado. (Entre el dieciséis y el cincuenta por ciento.)

Ampliamente Alcanzado (AA), indica el grado de alcance cuando la afirmación es cierta en gran medida. (Entre el cincuenta y uno y el ochenta y cinco por ciento.)

Completamente Alcanzado (CA). Cuando la afirmación es cierta casi en su totalidad o en su totalidad. (Entre el ochenta y seis y el cien por cien.)

Se incluye también un quinto nivel, **PO (Proceso Omitido),** si la afirmación evaluada no es cierta. (Cero por ciento.)

Mediante el uso del marco PEMM se van a obtener cinco niveles de madurez, del 0 al 4, donde el nivel PO del proceso corresponderá al nivel 0 de madurez del proceso; NA equivaldrá al nivel 1 de madurez del proceso, PA al nivel 2, AA al nivel 3 y CA, al nivel 4 de madurez del proceso.

El cálculo del nivel de madurez del proceso evaluado se obtendrá a partir del resultado del alcance de los facilitadores de dicho proceso, por ejemplo, si los cinco facilitadores de un proceso están en el nivel NA, el proceso está en el nivel NA; si los cinco facilitadores están en el nivel PA, el proceso está en el nivel PA. Sin embargo, si sólo cuatro de los cinco facilitadores suben a un determinado nivel, no se puede decir que el proceso haya logrado ese nivel; pertenece al de nivel inferior.

Este modelo tal y como está definido no podemos aplicarlo directamente, necesitamos un modelo de madurez de seis niveles (del 0 al 5), que son los que se han definido para evaluar el nivel de madurez de la organización y la capacidad de los procesos. Con este fin, se ha definido la siguiente operativa de cálculo del nivel de madurez de un proceso:

- En primer lugar, se asigna a cada nivel de alcance, de forma auxiliar, un valor equivalente, tal y como se indica en la siguiente tabla (Tabla 5):

Nivel Alcance	**Valor**
PO (Proceso Omitido).	Valor 0
NA (No Alcanzado).	Valor 1
PA (Parcialmente Alcanzado).	Valor 2
AA (Ampliamente Alcanzado).	Valor 3
CA (Completamente Alcanzado).	Valor 4

Tabla 5. Equivalencia Nivel de Alcance - Valor.

- Dado que cada facilitador va a incluir dos o tres cuestiones a evaluar, el nivel del facilitador se va a obtener a partir del valor -nivel de alcance- asignado a las cuestiones (ver Tabla 6):

- Si todas las cuestiones del facilitador tienen el mismo alcance (Valor N), ese será el nivel del facilitador.
- Si las cuestiones tienen asignado distinto nivel de alcance, es decir, distinto valor, el nivel del facilitador será el de valor inferior. (Donde valor N-2 es cualquier valor distinto e inferior a N-1; y N-1 es cualquier valor distinto e inferior a N).
- Para los facilitadores con tres cuestiones se añade un supuesto más, si dos de las tres cuestiones coinciden en valor, ese será el valor que determine el nivel del facilitador.

Número de cuestiones del facilitador	**Valor de cada cuestión**	**Resultado (Nivel del facilitador)**
3	Valor N	Valor N
	Valor N	
	Valor N	
	Valor N-1	Valor N
	Valor N	
	Valor N	
	Valor N-1	Valor N-1
	Valor N-1	
	Valor N	
	Valor N-2	Valor N-2
	Valor N-1	
	Valor N	
2	Valor N	Valor N
	Valor N	
	Valor N-1	Valor N-1
	Valor N	

Tabla 6. Obtención del nivel de un facilitador.

- Por último, a partir del nivel de los facilitadores se obtendrá el nivel de madurez del proceso. Se analiza en primer lugar si se cumplen los requisitos para obtener un nivel 5 de madurez; si no se cumplen, se valora si cumple las condiciones para el nivel 4 de madurez y así sucesivamente de forma decremental hasta llegar al nivel 0 de madurez. En la siguiente tabla (Tabla 7) está detallado el cálculo:

Número facilitadores con Valor 4	**Nivel de madurez del proceso**
5 facilitadores con Valor 4.	5
3 facilitadores con Valor 4; 2 con Valor 3.	4

Número facilitadores con Valor 3 o Valor 2	**Nivel de madurez del proceso**

5 facilitadores con Valor N. (N=2 o N=3)	Valor N
[1,4] facilitadores con Valor N; resto con cualquier Valor N<> [0,1]. (N=2 o N=3)	Min (Valor N)

Número facilitadores con Valor 1	**Nivel de madurez del proceso**
5 facilitadores con Valor 1.	1
3 facilitadores con Valor 1; 2 con Valor 0.	1
[1 ,4] facilitadores con Valor 1; resto con cualquier Valor N<>0.	1

Número facilitadores con Valor 0	**Nivel de Madurez del proceso**
5 facilitadores con Valor 0.	0
[3,4] facilitadores con Valor 0; 2 con cualquier Valor N.	0

Tabla 7. Cálculo nivel de madurez por proceso.

Una vez evaluado el nivel de madurez de todos los procesos, se podrá determinar el nivel de madurez de cada uno de los seis principios del estándar UNE-ISO/IEC 38500:

- Si todos los procesos que componen el principio tienen el mismo nivel de madurez, ese será el nivel de madurez del principio.
- Si los procesos tienen distinto nivel de madurez:
  - Si la mitad más uno, de los procesos coinciden en valor, ese será el nivel de madurez que se le asigne al principio.
  - Si esta regla no se cumpliera, el nivel de madurez se obtendrá calculando el menor de los niveles de madurez de los procesos que apoyan al principio. Salvo que el nivel inferior fuera cero, entonces se cogería el siguiente nivel mínimo superior. (Se define como norma propia que un principio será nivel cero solo si se cumplen los primeros supuestos, es decir, o todos o la mitad más uno de los procesos, tienen nivel de madurez cero.)

3.2.3 Gestión de los riesgos, seguridad y control T.I

Las organizaciones no pueden controlar todos los riesgos existentes, tanto por el coste que supone como por la dificultad de prevenir y conocer todas las amenazas por las que pueden verse afectadas, en su lugar suele definirse el nivel de seguridad que se pretende alcanzar, o dicho de otra manera, cuál es el nivel de riesgo relacionado con las tecnologías de la información que puede asumir la empresa sin que provoque interrupciones en los procesos o en los servicios ofrecidos, sobrecostes en T.I o la pérdida de ganancias. **[65]**

La identificación y la evaluación de los riegos deberían ser los primeros pasos que la Dirección debiera tomar para la gestión de los riesgos, para su control y eliminación.

En el proyecto, la evaluación de riesgos se realizará a través de un cuestionario sobre las siguientes áreas: la gestión de la Dirección sobre las T.I, el papel estratégico de las T.I y

sobre los principios del estándar UNE-ISO/IEC 38500. Cada pregunta tendrá cuatro opciones de respuesta **[71]:**

- Sí: cuando la cuestión planteada es cierta.
- No: si no lo es.
- No Aplica: si la cuestión no aplica a la entidad que se está evaluando.
- No Sabe / No Contesta: si no se conoce la respuesta.

Como resultado de la evaluación obtendremos los riesgos potenciales asociados (a cada pregunta contestada con un "no") y se propondrán los controles correspondientes para mitigarlos.

3.2.4 Implantación de Gobierno T.I

En este apartado se va a realizar una propuesta para la implantación de Gobierno T.I mediante la norma UNE-ISO/IEC 38500. Nuestro modelo, basado en las indicaciones planteadas por Alan Calder y Steve Moir **[16];** y en los pasos definidos para la implantación del gobierno de las T.I en las universidades **[65],** estará formado por las siguientes fases:

- Evaluación del gobierno T.I.
- Definir una hoja de ruta.
- Diseñar un plan de implantación.
- Implantación y seguimiento.

3.2.4.1 Formación inicial del gobierno T.I

Para que la implantación tenga éxito es importante que esté respaldada por la alta dirección, por lo que en ocasiones suele ser necesaria una etapa de formación para darles a conocer los fundamentos de gobierno de las T.I.

En esta primera etapa también habría que:

- Mostrar al Comité de Dirección las ventajas del gobierno T.I y presentarles el modelo de gobierno.
- Establecer un equipo de dirección, si no existe. Y si existiera, analizar la estructura de gobierno para determinar si los conocimientos del comité de dirección, su jerarquía de decisiones, etc., son las adecuadas.
- Identificar los elementos críticos que el gobierno T.I va a abordar.
- Elaborar un plan de implementación e identificar cuáles de esas tareas están ya implementadas en la organización.
- E identificar los recursos necesarios.

3.2.4.1 Definir una hoja de ruta

En la hoja de ruta se definen las necesidades de la organización, se analiza su situación actual en relación al gobierno T.I y se establecen las metas a alcanzar, es decir, dónde estamos ahora y dónde queremos llegar.

Para determinar "dónde estamos ahora", la Dirección debe saber cuál es la capacidad de la entidad y tener identificados los puntos débiles. Este análisis se realizará a través de la evaluación de los niveles de madurez de los procesos, que permitirá obtener el nivel de madurez de gobierno T.I actual en base a la norma UNE/ISO-IEC 38500.

3.2.4.2 Gestión de riesgos

Es importante identificar los distintos riesgos T.I que pueden afectar a la entrega de valor. Esta tarea se realizará mediante el cuestionario de riesgos.

En base al estado actual en el que se encuentra la organización, obtenido en la fase anterior, junto con el estado futuro que pretende alcanzar y los riesgos detectados, se pueden identificar las deficiencias en temas de gobierno T.I respecto a las mejores prácticas; lo que va a permitir poder establecer un plan de cambios para gestionar los riesgos detectados y alinear la estrategia de negocio y la estrategia T.I.

3.2.4.3 Diseñar un plan de implantación

El objetivo del plan es conocer aquellos mecanismos que posibiliten a la organización el alcance de las metas de acuerdo a lo definido en la hoja de ruta. En su diseño hay que tener en cuenta cuáles son las prioridades de la entidad, por ejemplo, si desea mejorar la eficiencia de sus operaciones o evitar los riesgos, los recursos disponibles y el capital dispuesto a invertir.

El plan debe también asegurar que todas las aplicaciones, software, hardware, etc., cuentan con un plan de gestión de ciclo de vida que comprende la etapa de desarrollo o inclusión al proyecto hasta su retirada u obsolescencia. Además, se debe incluir la documentación correspondiente de cada una de las etapas: los requisitos funcionales, técnicos, el diseño de la arquitectura a utilizar y los planes de implantación y pruebas en los diferentes entornos. (En base a la experiencia propia, esta tarea suele ser omitida en la mayoría de las entidades o proyectos, pues se da prioridad al desarrollo y la documentación suele ser un añadido que se realiza siempre al final, si hay margen de tiempo, y cuya realización depende la mayoría de las veces de las buenas prácticas de la persona responsable. La documentación debería constituir una fuente de datos.)

En la práctica, la identificación de los procesos a optimizar para mejorar el nivel de madurez de los principios de gobierno T.I, se obtendrá a partir de la evaluación del nivel de capacidad de los procesos descritos en nuestro modelo de autoevaluación. Las medidas preventivas también las proporciona el modelo, previo a la realización del cuestionario de riesgos.

3.2.4.3 Implantación y seguimiento

En esta última fase se desarrolla el plan de implementación de gobierno T.I planteado y se comprueba que los servicios diseñados e implantados cumplen con las especificaciones definidas. Para ello hay que monitorizar la eficiencia de los procesos y reportar los resultados al consejo de gobierno y a las partes interesadas, para que puedan realizar el seguimiento y valorar si hay alguna desviación respecto a la hoja de ruta, y si procediera, determinar e implantar las medidas de acción correspondiente.

Ninguna actividad o proceso es nunca eficiente al cien por cien, por lo que cada determinado tiempo debería volver a realizarse una evaluación del gobierno para identificar y optimizar los procesos que le dan soporte.

3.3 Auditoría y control según la norma UNE-ISO/IEC 38500:2013 – cuestionario de autoevaluación

La finalidad del cuestionario es proporcionar a los auditores, tanto internos como externos, a los consejeros o a cualquier persona con responsabilidad sobre las Tecnologías de la Información (bien en su evaluación, monitorización o gestión), una herramienta que les posibilite determinar el estado del marco de Gobierno Corporativo de las T.I en base a las indicaciones y recomendaciones definidas en la norma UNE-ISO/IEC 38500:2013. El cuestionario podrá ser utilizado para evaluar cualquier organización, independientemente del tipo, tamaño o sector al que pertenezca.

La estructura del cuestionario de autoevaluación que se propone, en base a las soluciones expuestas en el punto 3.2, quedaría definida de la siguiente forma (Figura 13):

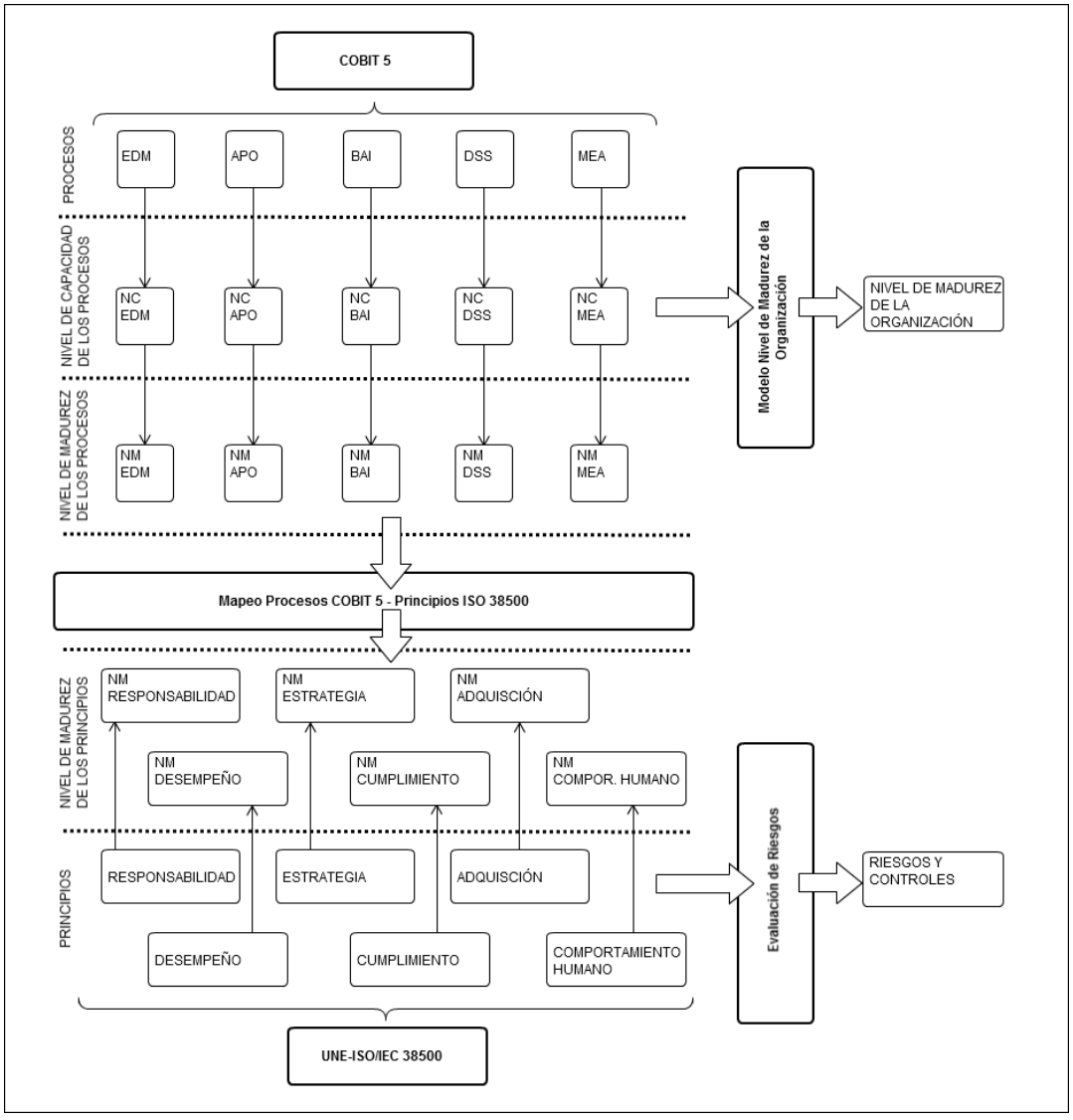

Figura 13. Esquema del cuestionario de autoevaluación.

A modo de resumen, según lo especificado:

- Se evalúan el nivel de capacidad y el nivel de madurez de los procesos de COBIT 5 (solamente los que dan soporte el estándar UNE-ISO/IEC 38500:2013). No hay un orden de ejecución predefinido para estas dos evaluaciones, pueden realizarse según la conveniencia del usuario.
- Con los niveles de madurez de los procesos y a través del correspondiente mapeo con los principios de la norma UNE-ISO/IEC 38500, se obtendrá el nivel de madurez de cada principio.

Aunque la finalidad del cuestionario es evaluar el uso de la T.I en una organización según la norma UNE-ISO/IEC 38500, la estructura definida nos permite, además:

- A partir del nivel de capacidad de los procesos y mediante el modelo del nivel de madurez de la organización, obtener el nivel de madurez correspondiente de la organización que se esté evaluando.
- Determinar las tareas a realizar para mejorar cada uno de los principios de la norma. ¿Cómo?, optimizando el conjunto de procesos que los sustentan, aquellos que tengan un nivel de capacidad bajo.
- Identificar, mediante el cuestionario adicional de evaluación de riesgos, los riesgos para cada uno de los principios del estándar y las medidas preventivas a realizar.

En este punto, además de la especificación de las preguntas que conforman los distintos cuestionarios, se incluye el diseño de un prototipo web que de soporte a la solución propuesta, incluida la generación de resultados correspondientes en base a la lógica definida en los puntos anteriores. El nombre que se propone para la aplicación es "AyCTI" (Análisis y Control de las Tecnologías de Información) y la funcionalidad que debe contemplar es la siguiente:

- Antes de comenzar el usuario debe revisar y completar los **datos** referentes a la **organización** a evaluar.
- Dispondrá de una opción donde podrá consultar el **histórico** de evaluaciones realizadas y un **comparador** de resultados.
- Podrá realizar una **nueva evaluación**, es decir, evaluar el nivel de capacidad de los procesos, el nivel de madurez de los mismos y realizar el cuestionario de riesgos.
- La última opción le permitirá **consultar** los **resultados** del nivel de capacidad y de madurez de cada proceso, consultar los riesgos y controles, el nivel de madurez de la organización y el nivel de madurez de los principios definidos en la norma UNE-ISO/IEC 38500.

Cada organización podrá decidir si la autoevaluación, constituida por los distintos tipos cuestionarios, es realizada por un auditor interno o uno externo, así que estos serán los roles principales de la aplicación. Además, se define el siguiente supuesto: una organización puede tener una o varias sedes y en cada sede siempre habrá designada una persona perteneciente a ella, que será la responsable de la T.I y por tanto en caso de la auditoría interna, quien lleve a cabo la evaluación.

Va a existir también una diferencia de funcionalidad respecto a estos dos roles. Estas cuestiones se detallarán en los puntos correspondientes en los que se describe la funcionalidad de la herramienta o aplicación.

3.3.1. Datos de la organización

En esta opción el usuario debe completar o validar los siguientes campos según corresponda:

Nombre o razón social.
Centro/Sede.

País.
Provincia a la que pertenece la empresa.
Tipo de organización.
Tamaño de la organización.
Industria en la que opera la empresa.
Facturación de la organización.

Inversión en T.I en el último año.
Inversión en T.I hace dos años.
Inversión en T.I hace tres años.

Tabla 8. Campos de la organización a revisar en la aplicación.

Como el auditor interno está vinculado a una única sede de una organización, los datos relativos al *Nombre*, *Centro*, *País*, *Provincia* estarán informados cuando el usuario acceda a la aplicación y no serán modificables. El resto de campos sí serán editables, teniendo que elegir un valor entre un conjunto de valores predefinidos.

El auditor externo por su parte deberá elegir la organización y sede a evaluar, pudiendo dar de alta una nueva organización y sede si se tratase de la primera evaluación a realizar sobre la organización y/o alguna de sus sedes. También podrá consultar y modificar los datos relativos a una organización o sede ya registrada.

La gestión de usuarios, así como la eliminación de datos relativos a las entidades o a los cuestionarios, no se podrán realizar desde la aplicación, esta funcionalidad será externa y sería delegada vía SLA (acuerdo de nivel de servicio) a la empresa encargada del mantenimiento software de la herramienta.

Comentar también que actualmente los campos de esta opción están definidos acorde con la división territorial española. En versiones futuras de la aplicación podrían ampliarse los campos definidos, para poder incluir las correspondientes divisiones territoriales de otros países.

3.3.2. Histórico

3.3.2.1 Histórico

En *Histórico* el usuario podrá consultar el listado de todas las evaluaciones realizadas en un rango de fechas que elija. Si se tratase del auditor externo tendrá que elegir además la sede y la organización que desea listar.

Se mostrará por cada sede, la fecha de inicio y fin de la evaluación junto con el identificador de la evaluación. Además, por cada evaluación se mostrará una fila por cada uno de los cuestionarios (nivel de capacidad, nivel de madurez de los procesos y riesgos) y mediante el estado se determinará si están o no completos. Un cuestionario estará completo si se han evaluado todos los procesos que engloba -en el caso de la evaluación para determinar el nivel de madurez o de capacidad- o en el caso de los cuestionarios de riesgos, si están informadas todas las preguntas.

Fecha inicio de la evaluación.
Fecha fin de la evaluación.
Identificador de la evaluación.
Tipo de cuestionario.
Identificador de cuestionario.
Estado.
Organización.
Sede.

Tabla 9. Campos definidos en la consulta por histórico.

Junto a cada cuestionario se habilitará un botón “Completar” que permitirá finalizar aquellos cuestionarios que no lo estuvieran.

Por buenas prácticas, se recomienda al usuario que antes de comenzar una evaluación nueva compruebe si tiene alguna pendiente.

3.3.2.2 Comparador

El comparador va a permitir contrastar los resultados de distintas evaluaciones, de los pares organización/sede seleccionados, en un rango de fechas determinado. En el caso del auditor interno solo podrá comparar los resultados de su propia organización.

Los resultados se van a mostrar por tipo de cuestionario. Como pueden existir cuestionarios para los que no se han evaluado todos los procesos, se va a añadir un filtro para determinar si se quieren o no incluir en los resultados los cuestionarios incompletos.

Para los cuestionarios de nivel de capacidad y madurez, el comparador mostrará el valor del nivel correspondiente obtenido por cada proceso (ver Tabla 10). Para el resultado de

la ISO38500 se mostrará el nivel de madurez de cada uno de los principios (ver Tabla 11); y por último, para el nivel de madurez de la organización se indicará el nivel alcanzado (ver Tabla 12).

En esta opción no se van a poder visualizar los valores informados en los cuestionarios, para ello se habilitará, dentro de la opción *Histórico*, esta funcionalidad a partir del cuestionario seleccionado.

Se muestran a continuación las tablas mencionadas:

Fecha inicio de la evaluación	Fecha fin de la evaluación	Id de la evaluación	Id del cuestionario	Proceso EDMO1	Proceso EDMO2	…	Proceso MEA03	Sede	Organización

Tabla 10. Tabla del comparador para N. Capacidad y Madurez por procesos.

Fecha inicio de la evaluación	Fecha fin de la evaluación	Id de la evaluación	Id del cuestionario	Principio 1 Responsabilidad	Principio 2 Estrategia	…	Principio 6 C. Humano	Sede	Organización

Tabla 11. Tabla del comparador para N. Madurez ISO 38500.

Fecha inicio de la evaluación	Fecha fin de la evaluación	Id de la evaluación	Id del cuestionario	N. Madurez de la organización	Sede	Organización

Tabla 12. Tabla del comparador para N. Madurez de la organización.

En versiones futuras podría completarse la funcionalidad permitiendo al auditor externo comparar más de dos organizaciones. También podrían añadirse gráficos para equiparar los resultados.

Si en algún momento se manejara un volumen elevado de datos otra opción de mejora sería integrar la aplicación con algún módulo de desarrollo de Big Data, por ejemplo, Apache Hadoop, o con alguna herramienta de Business Intelligence (B.I), como puede ser QlikView que cuenta con una opción de descarga gratuita. Para futuras versiones también podría plantearse desarrollar la aplicación Java utilizando el marco de trabajo JSF y la librería ICEfaces, pues además de facilitar y simplificar el desarrollo, permiten el funcionamiento correcto de la aplicación en distintos sistemas operativos sin necesidad de modificar el código fuente.

3.3.3 Nueva evaluación

Cada evaluación nueva que se realice engloba los siguientes cuestionarios:

- Nivel de capacidad de los procesos.
- Nivel de madurez de los procesos.
- Riesgos sobre la gestión de la Dirección sobre las T.I, el papel estratégico de las T.I y sobre los principios del estándar UNE-ISO/IEC 38500.

3.3.3.1 Nivel de capacidad de los procesos

Este cuestionario va a estar formado por un conjunto de preguntas agrupadas por proceso y por nivel de capacidad. Las cuestiones correspondientes a los niveles 0 y 1 de capacidad son específicas de cada proceso, mientras que las del resto de niveles son genéricas.

Por ejemplo, para los procesos del dominio Evaluar, Orientar y Supervisar (EDM) se muestran a continuación las preguntas para el Nivel 0 y el Nivel 1:

Niveles de capacidad							Procesos COBIT EDM				
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3 (Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)	**Cuestionario**	EDM01	EDM02	EDM03	EDM04	EDM05
						La empresa no necesita elaborar procesos de gobierno T.I.	x	x	x	x	x
						No existe ningún proceso relativo al gobierno T.I.	x	x	x	x	x
						No existen procesos para desarrollar o implantar el marco de gobierno T.I.	x				
						No se alcancza el valor óptimo de las iniciativas T.I, los servicios y los activos.	x				
						El modelo de toma de decisiones estratégico para T.I es eficaz y está alineado estrategia empresarial y con las exigencias de las partes interesadas (stakeholders).	x				
						El sistema de gobernanza para T.I está integrado en la empresa.	x				
						El sistema de gobernanza T.I funciona con eficacia.	x				
						No existen procesos que aseguren la entrega de beneficios.		x			
						La empresa asegura el valor óptimo de su cartera de proyectos o inversiones mediante iniciativas T.I, servicios y activos.		x			
						Se garantiza el valor óptimo de la inversión T.I a través de prácticas de gestión de valor efectivas.		x			
						La inversión T.I contribuye a incrementar el valor de negocio.		x			
						No existen procesos que aseguren la optimización del riesgo.			x		
						Están identificados los umbrales de riesgo y se conocen los principales riesgos asociados a las T.I.			x		
						La empresa gestiona los riegos críticos vinculados con las T.I de manera eficaz y eficiente.			x		
						No existen procesos que aseguren la optimización de recursos.				x	
						Los recursos que necesita la empresa están cubiertos de manera óptima.				x	
						Los recursos se asignan en base a las prioridades empresariales y siempre dentro de los límites presupuestados.				x	
						Se logra un uso óptimo de los recursos mediante ciclos de vida económicos completos.				x	
						No existen procesos que aseguren la transparencia de las partes interesadas.					x
						Los informes presentados por las partes interesadas están en línea con los requisitos definidos por los mismos.					x
						Los informes que se presentan son completos, se entregan a tiempo y son exactos.					x
						La comunicación es eficaz y las partes interesadas (stakeholders) están satisfechas.					x

Figura 14. Cuestiones Nivel de Capacidad EDM.

El cuestionario completo para la evaluación de todos los procesos está definido en el Anexo III "Cuestionario Nivel de Capacidad".

A continuación, se detallan las preguntas correspondientes para el resto de niveles, que como se ha comentado, son comunes a todos los procesos:

Niveles de capacidad							Procesos COBIT 5				
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3 (Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)		Dominio EDM	Dominio AP0	Dominio BAI	Dominio DSS	Dominio MEA
						Cuestionario					
						Están identificados los requisitos de desarrollo del proceso.	x	x	x	x	x
						Las tareas de desarrollo del proceso están planificadas y son supervisadas.	x	x	x	x	x
						El comportamiento del proceso se ajusta a la funcionalidad establecida.	x	x	x	x	x
						Los roles y responsabilidades relativas al proceso han sido establecidas y comunicadas.	x	x	x	x	x
						El proceso cuenta con la información y los recursos necesarios para su desarrollo.	x	x	x	x	x
						Existe un canal de comunicación eficaz entre las partes implicadas de cada proceso.	x	x	x	x	x
						Están identificadas las salidas del proceso.	x	x	x	x	x
						Están identificados los requisitos de documentación y de control de las salidas del proceso.	x	x	x	x	x
						Las salidas de los procesos están correctamente identificadas, documentadas y controladas.	x	x	x	x	x
						Las salidas del proceso se ajustan a los requerimientos definidos.	x	x	x	x	x
						Existe un proceso estándar que define los elementos fundamentales que deben ser incorporados en el proceso definido.	x	x	x	x	x
						En el estándar está definida la relación e interactuación del proceso con otros procesos.	x	x	x	x	x
						Los roles y las responsabilidades están también incluidas en el proceso estándar.	x	x	x	x	x
						La infraestructura requerida está definida en el proceso estándar.	x	x	x	x	x
						Está monitorizado el proceso para comprobar su	x	x	x	x	x

						nivel de efectividad y adecuación.					
						El proceso se despliega en base al proceso estándar.	x	x	x	x	x
						Se asignan al proceso, los roles, responsabilidades y autoridades requeridas.	x	x	x	x	x
						Los recursos que desarrollan el proceso son competentes y tienen la formación necesaria para llevar a cabo esta tarea.	x	x	x	x	x
						La infraestructura necesaria para el desarrollo del proceso está disponible y se realizan tareas para su mantenimiento y actualización.	x	x	x	x	x
						El proceso está documentado e incluye la forma en la que el proceso apoya los objetivos de negocio.	x	x	x	x	x
						Los objetivos o indicadores para medir el proceso se obtienen a partir de las necesidades de información del proceso.	x	x	x	x	x
						Se definen los objetivos cuantitativos para el funcionamiento de proceso utilizando como base los objetivos relevantes de negocio.	x	x	x	x	x
						Están identificados los criterios y la frecuencia de medición, así como los objetivos a medir para el funcionamiento del proceso.	x	x	x	x	x
						Los resultados de las mediciones son recogidos, analizados y reportados con el fin de monitorizar los objetivos para asegurar el funcionamiento de proceso.	x	x	x	x	x
						Los resultados de las mediciones son usados para determinar el funcionamiento de proceso.	x	x	x	x	x
						Se han definido técnicas de control y análisis para el proceso y estas son las que se utilizan.	x	x	x	x	x
						Están establecidos los límites de variación de los resultados de las mediciones, dentro de los cuales se asegura el funcionamiento normal del proceso.	x	x	x	x	x
						Los datos de las mediciones realizadas en el proceso se analizan para determinar el origen de las variaciones anormales.	x	x	x	x	x
						Si el resultado de la medición del proceso está fuera de los márgenes de variación establecidos, se llevan a cabo acciones correctivas.	x	x	x	x	x
						Cuando se aplica una acción correctiva sobre un proceso se garantiza que el proceso sigue funcionado correctamente y que, ahora, sus resultados están dentro de los márgenes de valores correctos.	x	x	x	x	x

						Los objetivos de mejora del proceso se establecen en base a los objetivos más relevantes del negocio.	x	x	x	x	x
						Están recopiladas las causas comunes que originan variaciones en el funcionamiento de proceso. Existe un proceso continuo de análisis de datos para identificar estas causas.	x	x	x	x	x
						Existe una tarea continua de análisis de datos para mejorar y poder introducir innovaciones en el proceso.	x	x	x	x	x
						Se analizan e identifican aquellas tecnologías y desarrollos que pueden optimizar el proceso.	x	x	x	x	x
						Existe un proceso de mejora continua.	x	x	x	x	x
						Los cambios propuestos son evaluados para ver si generan impacto sobre la funcionalidad y finalidad del proceso.	x	x	x	x	x
						Está identificada cualquier interrupción, que afecte al funcionamiento normal del proceso, originada por la implementación de cualquier cambio. Existe un mecanismo de contingencia para recuperar la normalidad del proceso.	x	x	x	x	x
						Tras la implementación de un cambio en el proceso se evalúa la eficacia del mismo, para determinar si los resultados obtenidos son debidos al cambio o a alguna causa especial.	x	x	x	x	x

Tabla 13. Cuestiones Nivel de Capacidad genéricas.

Para cada cuestión, según lo definido en el punto *3.2.2.1 Evaluación del nivel de capacidad de los procesos*, el usuario debe definir su grado de alcance, recordemos:

- No Alcanzado (NA). Si apenas hay evidencia del logro del objetivo. (Un porcentaje de grado de alcance entre el 0 y el 15%).
- Parcialmente Alcanzado (PA). Si se cumplen menos de la mitad de los objetivos del proceso. (Un porcentaje de grado de alcance comprendido entre el 16 y el 50%).
- Ampliamente Alcanzado (AA). Cuando, salvo por algunas deficiencias, se cumplen casi la totalidad de los objetivos del proceso evaluado. (Un porcentaje de grado de alcance que varía entre el 51 y el 85%).
- Completamente Alcanzado (CA). Se logran de manera completa los objetivos y no hay evidencias de debilidades. (Un porcentaje de grado de alcance cuyo valor oscila entre el 86 y el 100%).

Una vez evaluado y revisado cada proceso, el usuario debe confirmar los cambios (solo se podrá guardar la evaluación de un proceso si se han informado todos los supuestos). El resultado del nivel de capacidad de cada proceso podrá consultarse al finalizar su

evaluación y estará disponible en la sección *Resultados* de la aplicación, donde se mostrarán en forma de una tabla resumen.

3.3.3.2 Nivel de madurez de los procesos

La evaluación del nivel de madurez se realiza por proceso, donde las cuestiones están agrupadas por facilitador y por nivel de alcance, y son comunes a todos los procesos.

Por cada uno de los facilitadores descritos:

- ejecutores/desarrolladores,
- responsable,
- infraestructura,
- indicadores,

el usuario debe valorar cada una de las afirmaciones definidas y determinar su grado de alcance, tal y como se definió en el punto *3.2.2.3 Evaluación del nivel de madurez de los procesos:*

- Proceso Omitido (PO): La afirmación no es cierta. (0 por ciento).
- No Alcanzado (NA): La afirmación en gran medida no es cierta. (Entre el 1 y el 15 por ciento).
- Parcialmente Alcanzado (PA): La afirmación es cierta en cierto grado. (Entre el 16 y el 50).
- Ampliamente Alcanzado (AA): La afirmación es cierta en gran medida. (Entre el 51 y el 85 por ciento).
- Completamente Alcanzado (CA): La afirmación es cierta casi en su totalidad o en su totalidad. (Entre el 86 y el 100 por ciento).

Las preguntas que conforman el cuestionario de evaluación del nivel de madurez son las siguientes:

		Nivel de Alcance				Procesos COBIT 5				
Facilitador		No Alcanzado	Parcialmente Alcanzado	Ampliamente Alcanzado	Completamente Alcanzado	**EDM**	**AP0**	**BAI**	**DSS**	**MEA**
Diseño	Propósito	El proceso no se ha diseñado completamente.	El proceso se ha rediseñado completamente para cumplir su desempeño.	El proceso se ha diseñado para ajustarse a otros procesos y a la T.I de la empresa, optimizando así el desempeño de la empresa.	El proceso se ha diseñado para ajustarse a los procesos de los clientes y los proveedores, optimizando así el desempeño con las partes involucradas.	x	x	x	x	x
	Contexto	Están identificadas las entradas, salidas, los proveedores y los clientes del proceso.	Las necesidades de los clientes del proceso son conocidas y hay acuerdo sobre ellas.	Se definen las expectativas de desempeño cuando el proceso interactúa con otros procesos (las expectativas propias a cumplir y las esperadas de los otros procesos).	Las parte implicadas con los que interactúa un proceso, han definido sus expectativas de desempeño.	x	x	x	x	x
	Documentación	La documentación del proceso es principalmente funcional, pero identifica las interconexiones en la organización de las partes involucradas en la ejecución del proceso.	Hay documentación relativa al diseño del proceso.	La documentación del proceso describe las interacciones con otros procesos y las expectativas. También se define la relación del proceso con el sistema y la arquitectura de datos de la empresa.	En la documentación se definen los componentes necesarios que soportan el diseño del proceso.	x	x	x	x	x

Ejecutores/ Desarrolladores	Conocimiento	Los desarrolladores pueden identificar el nombre del proceso que están ejecutando e identificar los indicadores clave de su desempeño.	Los desarrolladores pueden describir el flujo global del proceso, el impacto del mismo y los niveles de desempeño real y requerido.	Los desarrolladores están familiarizados con los conceptos fundamentales del negocio de manera que pueden describir cómo su trabajo afecta a otros procesos y al desempeño de la empresa.	Los desarrolladores conocen las tendencias y el impacto de las mismas en la empresa.	x	x	x	x	x
	Destrezas	Los desarrolladores conocen los mecanismos de resolución de problemas que puedan surgir, así como los de cálculo de procesos.	Los desarrolladores trabajan en equipo y pueden autogestionarse.	Los desarrolladores tienen conocimiento y experiencia en la toma de decisiones de negocio que afecten al proceso.	Los desarrolladores tienen el conocimiento necesario para llevar a cabo la gestión de cambios del proceso.	x	x	x	x	x
	Conducta	Los desarrolladores se ajustan al proceso tratando siempre de cumplir la funcionalidad del mismo.	Los desarrolladores tratan de seguir el diseño del proceso, ejecutarlo correctamente y trabajar de manera que permitan a las personas involucradas en el proceso hacer eficazmente su trabajo.	Los desarrolladores se esfuerzan por asegurar que el proceso genera los resultados óptimos y esperados.	Los desarrolladores promueven la mejora continua del proceso.	x	x	x	x	x

Responsable	Identidad	El responsable del proceso está encargado de mejorar el desempeño del mismo.	Los responsables de la organización han creado un rol de responsable del proceso. La persona designada cumple con los requisitos para llevar a cabo las tareas del puesto.	El responsable prioriza las acciones necesarias para asegurar los tiempos y los objetivos del proceso.	El responsable pertenece al Consejo o al nivel organizativo más alto que se encarga de la toma de decisiones empresariales.	x	x	x	x	x

	Actividades	El responsable identifica y documenta el proceso, así como los cambios realizados, lo comunica a todas las partes involucradas.	El responsable comunica las metas del proceso y las mejoras que puedan realizarse, planifica su implementación y se asegura de que se cumpla el diseño del proceso.	El responsable colabora para facilitar la integración de los procesos y lograr así las metas de la empresa.	El responsable participa en la planificación estratégica del proceso para identificar iniciativas, mejoras, etc., del proceso.	x	x	x	x	x
	Autoridad	El responsable no tiene la autoridad suficiente para autorizar los cambios.	El responsable puede reunir a un equipo de rediseño de procesos e implementar el nuevo diseño. Tiene cierto control sobre el presupuesto de tecnología para el proceso.	El responsable conoce la T.I en la que se apoya el proceso y los proyectos que pueden afectar al proceso. Posee también cierta capacidad de decisión sobre los recursos y costes que se van a asignar al proceso.	El responsable controla totalmente el coste del proceso y tiene una gran capacidad de decisión sobre la asignación de recursos.	x	x	x	x	x

Infraestructura	Sistemas de información	El proceso está apoyado por la T.I.	El proceso está apoyado por la T.I creada a partir de los requisitos funcionales.	El proceso se apoya en un sistema integrado con la T.I y está ajustado a los estándares de la empresa.	El proceso se apoya en un sistema T.I con arquitectura modular y está ajustado a los estándares del sector de la empresa.	x	x	x	x	x
	Sistemas de recursos humanos	Se recompensa el logro de excelencia funcional y la resolución de problemas a nivel de proceso.	El diseño del proceso determina los roles y las responsabilidades así como la asignación de los mismos.	Los sistemas de contratación, desarrollo, reconocimiento y recompensa enfatizan las necesidades y los resultados del proceso.	Los sistemas de contratación, desarrollo, recompensa y reconocimiento refuerzan la importancia de la colaboración intra e interempresarial, el aprendizaje personal y el cambio organizacional.	x	x	x	x	x

Indicadores	Definición	Están definidos para el proceso los indicadores de coste y calidad.	Están definidos los costes del proceso, para todo el su ciclo vida, en base a los requisitos del cliente.	Los indicadores del proceso se han derivado de los objetivos estratégicos de la empresa.	Los indicadores del proceso se han derivado de las metas estratégicas del sector.	x	x	x	x	x
	Usos	Los ejecutivos usan los indicadores del proceso para monitorizar su desempeño, identificar las variaciones de desempeño e identificar mejoras.	Se usan los indicadores del proceso para comparar el desempeño actual con el desempeño esperado y en base al resultado, fijar los objetivos de desempeño.	Los ejecutivos presentan los indicadores a los desarrolladores de proceso para motivar y crear conciencia.	Los ejecutivos revisan y actualizan regularmente los indicadores y objetivos del proceso y los usan al planificar la estrategia de la empresa.	x	x	x	x	x

Tabla 14. Cuestionario de evaluación del Nivel de Madurez por proceso.

El cálculo del nivel de madurez del proceso será transparente para el usuario. Su resultado se mostrará en una tabla resumen en la sección *Resultados* de la aplicación. Esta tabla se irá actualizando cada vez que el usuario evalúe, revise y confirme la evaluación de cada proceso.

3.3.3.3 Riesgos

Este cuestionario no tiene una lógica de cálculo vinculada al resto de los cuestionarios, de manera que el usuario podrá evaluar los riesgos acerca de:

- la función del consejo de administración sobre las T.I,
- el papel de la función de T.I como factor estratégico del negocio,
- los principios de la norma UNE-ISO/IEC 38500,

de manera independiente, sin necesidad de haber realizado previamente alguna de las evaluaciones disponibles sobre los procesos.

El formulario de riesgos contiene tres tipos de cuestionarios, uno por cada área de evaluación de riesgos indicadas en el párrafo anterior. Cada cuestionario se compone de una serie de preguntas cuya respuesta admite las siguientes opciones: “Sí”, “No”, “No Aplica” o “No Sabe/No Contesta”. Solamente aquellas cuestiones que el usuario valore como no conforme, son las que se determinan como causa potencial de riesgo y, por tanto, serán sobre las que se muestren los riesgos de su no cumplimiento y los controles preventivos a aplicar para evitar su impacto y consecuencias.

Por ejemplo, para el principio de Adquisición de la norma UNE-ISO/IEC 38500 el cuestionario de riesgos sería el siguiente:

Principio de Adquisición - Cuestiones
¿La inversión T.I se realiza en base al análisis estratégico de la Dirección?
¿Se dispone de un Plan de Infraestructura Tecnológica?
¿Se realizan revisiones del plan de infraestructura tecnológica?
¿A la hora de elaborar la infraestructura tecnológica se tienen en cuenta las tendencias y la normativa aplicable?
¿Antes de adquirir una nueva tecnología se analiza su impacto?
¿Se tienen en cuenta aspectos como la adecuación, evolución, etc., de la infraestructura, en el plan tecnológico?
¿Se realizan y planifican tareas de mantenimiento tecnológico?
¿Existen un entorno de pruebas?
¿La Dirección interviene el las tareas de adquisición?

Figura 15. Ejemplo cuestionario riesgos.

El cuestionario completo para la evaluación de los riesgos está definido en el Anexo IV “Cuestionario de Riesgos”.

Una vez que el cuestionario ha sido completado y validado por el usuario, en la sección *Resultado* de la aplicación, se podrá ver el resultado con los riesgos y controles que apliquen.

Como futura mejora, de manera general para los diferentes cuestionarios podría incluirse un peso, por ejemplo, de 0 a 5 o de 0 a 10, de manera que el usuario en base a ese valor determinara la importancia en su organización de cada pregunta que conforma el cuestionario. El nivel correspondiente de cada proceso se calcularía teniendo en cuenta el peso asignado por el usuario y el grado de cumplimento de cada pregunta.

3.3.4 Resultados

Las opciones que se van a mostrar son los resultados de los siguientes cuestionarios:

- Cuestionario de nivel de capacidad de los procesos.
- Cuestionario de nivel de madurez de los procesos.
- Cuestionario de riesgos.
- Nivel de madurez de la organización.
- Nivel de madurez de los principios de la norma UNE-ISO/IEC 38500.

El acceso a los resultados correspondientes al nivel de madurez de la organización y al nivel de madurez de los principios de la norma UNE-ISO/IEC 38500, va a estar disponible, pero tal y como se ha definido en el esquema del cuestionario de autoevaluación, su valor va a depender de que se hayan completado los cuestionarios de nivel de capacidad y de nivel de madurez de los procesos.

3.3.4.1 Resultado - Nivel de capacidad de los procesos

Cada vez que el usuario evalúa y completa un proceso, puede consultar su resultado. El resultado del nivel de capacidad de cada proceso se mostrará en una tabla resumen, en la que se indicará el nombre del proceso y junto a él se mostrará el valor correspondiente obtenido.

Se ha decidido incluir en la tabla los procesos de COBIT 5 que no dan soporte a la norma UNE-ISO/IEC 38500. Así, si el auditor tiene nociones sobre COBIT 5 evita que llegue a pensar que tiene procesos pendientes por evaluar, que la aplicación esté incompleta o no funcione correctamente. Además, si en versiones futuras se extendiera la aplicación y se evaluaran todos los procesos de COBIT 5, minimizamos el número de cambios definiendo una estructura lo más genérica posible.

Los procesos no incluidos se distinguirán del resto a evaluar porque tendrán un estilo diferente. A continuación, se muestra un ejemplo de formato de la tabla resumen del resultado de la evaluación por nivel de capacidad, con los campos a incluir:

Procesos COBIT 5			Nivel de Capacidad
EDM			
Evaluar, Orientar y Supervisar.	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	
	EDM02	Asegurar la Entrega de Beneficios.	
	EDM03	Asegurar la Optimización del Riesgo.	
	EDM04	Asegurar la Optimización de los Recursos.	
	EDM05	Asegurar la Transparencia hacia las partes interesadas.	
AP0			
Alinear, Planificar y Organizar.	APO01	Gestionar el Marco de Gestión de TI.	
	APO02	Gestionar la Estrategia.	
	APO03	Gestionar la Arquitectura Empresarial.	
	APO04	Gestionar la Innovación.	
	APO05	Gestionar el portafolio.	
	APO06	Gestionar el Presupuesto y los Costes.	
	APO07	Gestionar los Recursos Humanos.	
	APO08	Gestionar las Relaciones.	
	APO09	Gestionar los Acuerdos de Servicio.	
	APO10	Gestionar los Proveedores.	
	APO11	Gestionar la Calidad.	
	APO12	Gestionar el Riesgo.	
	APO13	Gestionar la Seguridad.	
BAI			
Construcción, Adquisición e Implementación.	BAI01	Gestionar los Programas y Proyectos.	
	BAI02	Gestionar la Definición de Requisitos.	
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.	
	BAI04	Gestionar la Disponibilidad y la Capacidad.	
	BAI05	Gestionar la introducción de Cambios Organizativos.	
	BAI06	Gestionar los Cambios.	
	BAI07	Gestionar la Aceptación del Cambio y de la Transición.	
	BAI08	Gestionar el Conocimiento.	
	BAI09	Gestionar los Activos.	
	BAI10	Gestionar la Configuración.	
Entregar, dar Servicio	DSS01	Gestionar las Operaciones.	

y Soporte.	DSS02	Gestionar las Peticiones y los Incidentes del Servicio.	
	DSS03	Gestionar los Problemas.	
	DSS04	Gestionar la Continuidad.	
	DSS05	Gestionar los Servicios de Seguridad.	
	DSS06	Gestionar los Controles de los Procesos del Negocio.	
MEA			
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	

Tabla 15. Ejemplo formato tabla resumen del resultado de la evaluación por Nivel de Capacidad.

Cada vez que la evaluación de la capacidad de un proceso se confirme, la tabla se irá actualizando. Conseguimos así que no sea necesario concluir la evaluación de todos los procesos para consultar los resultados y que el usuario pueda acceder a ellos en cualquier momento.

3.3.4.2 Resultado - Nivel de madurez de los procesos

Cada vez que un usuario complete el cuestionario de nivel de madurez para un proceso, podrá consultar en esta sección el resultado de la evaluación. Es necesario dar valor a todas las preguntas, que componen cada cuestionario por proceso, para poder guardar los valores en el sistema y obtener su nivel de madurez. Si un usuario intenta guardar un cuestionario incompleto, existirá una validación que compruebe si todas las preguntas están informadas y si no se cumple este supuesto, mostrará un mensaje de error o advertencia. Esta regla se va a aplicar también al resto de formularios.

El resultado del nivel de madurez de cada proceso se mostrará en una tabla resumen, en la que se indicará el nombre del proceso y junto a él se mostrará el valor correspondiente obtenido. Al igual que se ha definido para el resultado del nivel de capacidad de los procesos se van a incluir todos los procesos de COBIT, estableciendo un estilo diferente para aquellos que no dan soporte a la norma ISO.

A continuación, se muestra un ejemplo de formato de la tabla resumen del resultado de la evaluación por nivel de madurez, con los campos a incluir:

Procesos COBIT 5			**Nivel de Madurez**
EDM			
Evaluar, Orientar y Supervisar.	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	

	EDM02	Asegurar la Entrega de Beneficios.	
	EDM03	Asegurar la Optimización del Riesgo.	
	EDM04	Asegurar la Optimización de los Recursos.	
	EDM05	Asegurar la Transparencia hacia las partes interesadas.	
AP0			
Alinear, Planificar y Organizar.	APO01	Gestionar el Marco de Gestión de TI.	
	APO02	Gestionar la Estrategia.	
	APO03	Gestionar la Arquitectura Empresarial.	
	APO04	Gestionar la Innovación.	
	APO05	Gestionar el portafolio.	
	APO06	Gestionar el Presupuesto y los Costes.	
	APO07	Gestionar los Recursos Humanos.	
	APO08	Gestionar las Relaciones.	
	APO09	Gestionar los Acuerdos de Servicio.	
	APO10	Gestionar los Proveedores.	
	APO11	Gestionar la Calidad.	
	APO12	Gestionar el Riesgo.	
	APO13	Gestionar la Seguridad.	
BAI			
Construcción, Adquisición e Implementación.	BAI01	Gestionar los Programas y Proyectos.	
	BAI02	Gestionar la Definición de Requisitos.	
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.	
	BAI04	Gestionar la Disponibilidad y la Capacidad.	
	BAI05	Gestionar la introducción de Cambios Organizativos.	
	BAI06	Gestionar los Cambios.	
	BAI07	Gestionar la Aceptación del Cambio y de la Transición.	
	BAI08	Gestionar el Conocimiento.	
	BAI09	Gestionar los Activos.	
	BAI10	Gestionar la Configuración.	
Entregar, dar Servicio y Soporte.	DSS01	Gestionar las Operaciones.	
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio.	
	DSS03	Gestionar los Problemas.	
	DSS04	Gestionar la Continuidad.	
	DSS05	Gestionar los Servicios de Seguridad.	

	DSS06	Gestionar los Controles de los Procesos del Negocio.	
MEA			
Supervisión, Evaluación y Verificación.	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	

Tabla 16. Formato tabla resumen del resultado de la evaluación por nivel de madurez.

3.3.4.3 Resultado - Riesgos

Los resultados estarán agrupados en los mismos bloques en los que se ha dividido el cuestionario de riesgos:

- Labor del consejo de administración sobre las T.I.
- Función de la T.I.
- Principios de la norma UNE-ISO/IEC 38500.

Cada vez que se complete y guarde uno de estos tres tipos cuestionarios, el usuario podrá consultar el resultado. El resultado se mostrará mediante una tabla resumen, que contiene aquellas preguntas con las que el usuario no estaba de acuerdo, junto con sus riesgos y los controles asociados. Por ejemplo, para el principio de Adquisición de la norma UNE-ISO/IEC 38500:

Cuestión	**Riesgos**	**Controles**
¿La inversión T.I se realiza en base al análisis estratégico de la Dirección?	• La T.I no se han dimensionado correctamente. • Los objetivos de negocio y los de T.I no están alineados	• Definición de los objetivos estratégicos. • Determinar las metas empresariales. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo.
¿Se dispone de un Plan de Infraestructura Tecnológica?	• Las exigencias de los usuarios se ejecutan con demora. • La falta de innovación T.I puede provocar la pérdida de oportunidades.	• Determinar las metas empresariales.
¿Se realizan revisiones del plan de infraestructura tecnológica?	• Las exigencias de los usuarios se ejecutan con demora. • La falta de innovación T.I puede provocar la pérdida de oportunidades.	• Determinar las metas empresariales. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias.

		• Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo. • Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario.
¿A la hora de elaborar la infraestructura tecnológica se tienen en cuenta las tendencias y la normativa aplicable?	• Capacidad de innovación limitada. • No se cumple con la normativa.	• Determinar las metas empresariales. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo. • Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario. • Conocer y seguir la normativa aplicable.
¿Antes de adquirir una nueva tecnología se analiza su impacto?	• Los sistemas actuales de la organización pueden ver afectado su funcionamiento tras la incorporación de una tecnología.	• Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario. • No realizar inversiones tecnológicas sin leer previamente los informes correspondientes.
¿Se tienen en cuenta aspectos como la adecuación, evolución, etc., de la infraestructura, en el plan tecnológico?	• Interrupción de los servicios. • Riesgo de quiebra de la entidad.	• Elaborar y mantener un plan para el mantenimiento la infraestructura tecnológica.

¿Se realizan y planifican tareas de mantenimiento tecnológico?	• Existen procesos claves que están sostenidos por tecnologías desfasadas.	• Elaborar y mantener un plan para el mantenimiento la infraestructura tecnológica. • Evaluar de forma periódica la infraestructura para conocer su estado.
¿Existen un entorno de pruebas?	• La omisión de pruebas puede provocar que, al implantar una aplicación en producción, se produzcan fallos o interrupciones en el servicio. • Al no realizar pruebas, no se garantiza el resultado de las aplicaciones.	• Definir un plan de pruebas, que garantice los resultados y la operatividad del sistema. • Las implantaciones en producción deben incluir una fase de pruebas en dicho entorno.
¿La Dirección interviene en las tareas de adquisición?	• Se realizar inversiones no alineadas con las necesidades del negocio.	• Elaborar un plan de adquisición.

Tabla 17. Formato tabla resumen del resultado de la evaluación por riesgos.

3.3.4.4 Resultado - Madurez de la organización

Mientras no se haya realizado de forma completa la evaluación del Nivel de Capacidad, es decir, mientras no se hayan evaluado todos los procesos, no se mostrará el resultado de la madurez de la organización.

El formato del resultado en este caso es muy simple, estará formado por un texto indicativo y el valor de madurez de la organización obtenido. Por ejemplo:

"El valor de madurez de la organización obtenido es: _____ "

Para versiones futuras de la aplicación, todas las operaciones que ahora mismo están contempladas dentro de la lógica de desarrollo de la aplicación y que se han definido para establecer los cálculos de los cuestionarios, podrían estar visibles, dando a conocer al usuario estos valores y los cálculos intermedios. Por ejemplo, la tabla equivalente a la "Tabla 4 - Procesos definidos por nivel de madurez" definida en el apartado "3.2.2.2 Evaluación del nivel de madurez de la organización", debería mostrar el valor del nivel de capacidad de cada proceso e indicar si, en base a los valores y a las reglas definidas, se alcanza el nivel de madurez en cuestión. El diseño de esta tabla podría ser el siguiente:

Nivel de madurez de la organización	**Procesos**	**Nivel Capacidad del proceso**	**Nivel madurez alcanzado (Sí/No)**
Nivel 0, Inmadura	No existen procesos definidos en este nivel.		
Nivel 1, Básica	BAI02. Gestionar la Definición de Requisitos.		
	BAI03. Gestionar la Identificación y la Construcción de Soluciones.		

	BAI07. Gestionar la Aceptación del Cambio y de la Transición.		
Nivel 2, Gestionada	APO01. Gestionar el Marco de Gestión de T.I.		
	APO02. Gestionar la Estrategia.		
	APO09. Gestionar los Acuerdos de Servicio.		
	APO10. Gestionar los Proveedores.		
	BAI01. Gestionar los Programas y Proyectos.		
	BAI06. Gestionar los Cambios.		
	DSS06. Gestionar los Controles de los Procesos del Negocio.		
Nivel 3, Establecido	APO03. Gestionar la Arquitectura Empresarial.		
	APO05. Gestionar el portafolio.		
	APO07. Gestionar los Recursos Humanos.		
	BAI05. Gestionar la introducción de Cambios Organizativos.		
	BAI08. Gestionar el Conocimiento.		
Nivel 4, Predecible	APO06. Gestionar el Presupuesto y los Costes.		
	APO12. Gestionar el Riesgo.		
	MEA01. Supervisar, Evaluar y Valorar Rendimiento y Conformidad.		
	MEA03. Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.		
Nivel 5, Optimizando	EDM01. Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.		
	EDM02. Asegurar la Entrega de Beneficios.		
	EDM03. Asegurar la Optimización del Riesgo.		
	EDM04. Asegurar la Optimización de los Recursos.		
	APO04. Gestionar la Innovación.		
	APO11. Gestionar la Calidad.		
	MEA02. Supervisar, Evaluar y Valorar el Sistema de Control Interno.		

Tabla 18. Visualización de la tabla *Procesos definidos por nivel de madurez*.

3.3.4.5 Resultado - Madurez de los principios de la UNE-ISO/IEC 38500

Aunque el acceso a esta sección va a estar siempre visible, los resultados relativos al nivel de madurez de cada principio de la norma UNE-ISO/IEC 38500 no van a visualizarse hasta que se haya completado el cuestionario de nivel de madurez para todos los procesos habilitados. (Para más detalle o a modo de recordatorio, acceder al punto "3.2.1.3 Adopción de la norma UNE- ISO/IEC 38500:2013" de la memoria, donde se ha definido cómo los procesos de COBIT 5 apoyan la norma y el mapeo entre ambos).

El resultado se mostrará en una tabla resumen, en la que se indicará el nombre del principio y junto a él se mostrará el valor correspondiente obtenido:

Principio de la UNE-ISO/IEC 38500	**Nivel del madurez del principio**
Responsabilidad	
Estrategia	
Adquisición	
Desempeño	
Cumplimiento	
Conducta humana	

Tabla 19. Formato tabla resumen del resultado de la madurez de los principios de la UNE-ISO/IEC 38500.

Otro ejemplo de tablas intermedias de cálculo a incluir en versiones futuras podría ser la indicada en la Tabla 20, en la que se detallan los procesos que dan soporte a cada principio, su nivel de madurez y en base a estos valores, el nivel de madurez global del principio:

Principio	**Proceso**		**Nivel de madurez del proceso**	**Nivel de madurez del principio**
Responsabilidad				
	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.		
	EDM02	Asegurar la Entrega de Beneficios.		
	EDM03	Asegurar la Optimización del Riesgo.		
	EDM04	Asegurar la Optimización de los Recursos.		
	EDM05	Asegurar la Transparencia hacia las partes interesadas.		
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
Estrategia				
	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.		
	EDM02	Asegurar la Entrega de Beneficios.		
	EDM03	Asegurar la Optimización del Riesgo.		
	APO01	Gestionar el Marco de Gestión de TI.		
	APO02	Gestionar la Estrategia.		
	APO03	Gestionar la Arquitectura Empresarial.		
	APO04	Gestionar la Innovación.		
	APO05	Gestionar el portafolio.		

	APO06	Gestionar el Presupuesto y los Costes.	
	APO07	Gestionar los Recursos Humanos.	
	APO11	Gestionar la Calidad.	
	APO12	Gestionar el Riesgo.	
	BAI01	Gestionar los Programas y Proyectos.	
	DSS06	Gestionar los Controles de los Procesos del Negocio.	
	EDM03	Asegurar la Optimización del Riesgo.	
	APO01	Gestionar el Marco de Gestión de TI.	
	APO05	Gestionar el portafolio.	
	APO06	Gestionar el Presupuesto y los Costes.	
	APO10	Gestionar los Proveedores.	
	APO11	Gestionar la Calidad.	
	APO12	Gestionar el Riesgo.	
	BAI01	Gestionar los Programas y Proyectos.	
	BAI02	Gestionar la Definición de Requisitos.	
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.	
	BAI05	Gestionar la introducción de Cambios Organizativos.	
	BAI06	Gestionar los Cambios.	
	BAI07	Gestionar la Aceptación del Cambio y de la Transición.	
	BAI08	Gestionar el Conocimiento.	
	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
Adquisición			
	EDM03	Asegurar la Optimización del Riesgo.	
	APO01	Gestionar el Marco de Gestión de TI.	
	APO05	Gestionar el portafolio.	
	APO06	Gestionar el Presupuesto y los Costes.	
	APO10	Gestionar los Proveedores.	
	APO11	Gestionar la Calidad.	
	APO12	Gestionar el Riesgo.	
	BAI01	Gestionar los Programas y Proyectos.	
	BAI02	Gestionar la Definición de Requisitos.	

	BAI03	Gestionar la Identificación y la Construcción de Soluciones.		
	BAI05	Gestionar la introducción de Cambios Organizativos.		
	BAI06	Gestionar los Cambios.		
	BAI07	Gestionar la Aceptación del Cambio y de la Transición.		
	BAI08	Gestionar el Conocimiento.		
	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.		
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
Desempeño				
	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.		
	EDM02	Asegurar la Entrega de Beneficios.		
	EDM03	Asegurar la Optimización del Riesgo.		
	EDM04	Asegurar la Optimización de los Recursos.		
	APO02	Gestionar la Estrategia.		
	APO05	Gestionar el portafolio.		
	APO09	Gestionar los Acuerdos de Servicio.		
	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad.		
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
Cumplimiento				
	EDM02	Asegurar la Entrega de Beneficios.		
	APO02	Gestionar la Estrategia.		
	APO05	Gestionar el portafolio.		
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.		
Conducta humana				
	EDM03	Asegurar la Optimización del Riesgo.		
	APO01	Gestionar el Marco de Gestión de TI.		
	APO07	Gestionar los Recursos Humanos.		
	APO11	Gestionar la Calidad.		
	BAI02	Gestionar la Definición de Requisitos.		
	BAI03	Gestionar la Identificación y la Construcción de Soluciones.		

	BAI05	Gestionar la introducción de Cambios Organizativos.	
	BAI08	Gestionar el Conocimiento.	
	DSS06	Gestionar los Controles de los Procesos del Negocio.	
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno.	

Tabla 20. Visualización de la tabla para el cálculo del nivel de madurez de los principios de la UNE-ISO/IEC 38500.

Capítulo 4
Planificación y presupuesto

Antes de comenzar cualquier proyecto hay que realizar una planificación previa para tener una estimación en cuanto al coste, los recursos, la duración del proyecto y poder analizar posibles desviaciones.

Por tanto, en este capítulo se van a especificar las tareas para llevar a cabo el proyecto, el esfuerzo de las mismas y los costes de los recursos necesarios.

Las fases que conforman el proyecto son las siguientes:

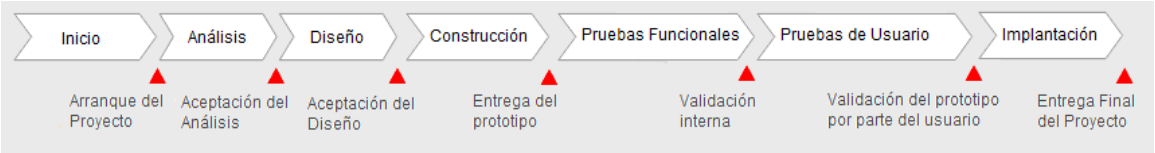

Figura 16. Fases del proyecto. **[72]**

En la fase **Inicio**, se define el objeto y alcance del proyecto y se recogen todos los requisitos que deben cumplirse: funcionales, sobre la duración del mismo, la metodología a seguir, etc.; También se identifican los posibles riesgos o dificultades, se definen los recursos necesarios y, por último, se define a alto nivel la solución general propuesta.

La fase de **Análisis** en este proyecto es la de mayor duración. Incluye toda la etapa de búsqueda de documentación relativa a las tecnologías de la información, gobierno T.I, consulta de las diferentes normativas, etc., y la propuesta propia de la estructura del cuestionario de autoevaluación como solución para la realización de auditoría y control del gobierno T.I en una organización.

Como el proyecto incluye la elaboración de un prototipo de aplicación que implemente el cuestionario de autoevaluación, la fase de **Diseño** comprende también las tareas de definición del entorno de desarrollo, el diseño de base de datos relacionales, el esquema de navegación, etc. Se elaboran, además, en esta fase todas las preguntas de cada uno de los cuestionarios y se definen los modelos y los cálculos necesarios para obtener los resultados.

Las fases de **Construcción y Pruebas** hacen referencia a la implementación y pruebas del prototipo de aplicación. El modelo de ciclo de vida software elegido es Incremental: este modelo se basa en la entrega de diversos prototipos en los que se va aumentando la funcionalidad implementada en cada uno de ellos. Aunque las primeras versiones no son un reflejo del producto final, sí tienen desarrollada la funcionalidad definida y requerida por el usuario para esa entrega. Además, este realizará las pruebas correspondientes para evaluar la aplicación, detectar errores o proponer cambios, que serán incorporados en los siguientes prototipos.

Una vez realizadas las pruebas correspondientes tiene lugar la fase de **Implantación**, que en este caso corresponde a la finalización del proyecto, entrega y presentación del mismo.

Se indican a continuación las tareas que comprende el proyecto:

Tarea
Inicio
Definición del alcance del proyecto.
Estimación del proyecto y de los recursos necesarios.
Elaboración de la propuesta de solución.
Análisis
Etapa de documentación.
Definición de los elementos del cuestionario de autoevaluación.

Diseño
Definición de la arquitectura del entorno de desarrollo.
Diseño de la solución propuesta.
Definición de los modelos y cálculos para obtener los resultados de los cuestionarios.
Elaboración de los cuestionarios.
Construcción
Desarrollo del prototipo del cuestionario de autoevaluación.
Pruebas Funcionales
Realización de pruebas internas.
Corrección de errores detectados.
Pruebas de Usuario
Realización de pruebas finales.
Implantación
Presentación y entrega del proyecto.

Tabla 21. Tareas del plan de trabajo.

Existe una tarea implícita en cada una de las fases, la elaboración de la documentación de la memoria del proyecto, que debe tenerse en cuenta en la elaboración de estimación. En el diagrama Gantt se representarán además de las tareas indicadas, mediante los hitos correspondientes, las entregas al tutor y las validaciones.

La estimación se ha elaborado en función del esfuerzo, es decir, las horas totales que llevaría completar cada tarea, de manera que la duración del proyecto en base a su planificación dependerá de los recursos disponibles y de la capacidad de los mismos. Asimismo, a cada tarea del plan de trabajo se ha asignado un nivel de complejidad, del uno al cinco, y en base a este se aplica un factor correctivo para calcular su esfuerzo total estimado, tal y como se muestra a continuación:

Tarea	**Complejidad**				
Análisis	A1	A2	A3	A4	A5
Factor Correctivo	0	0	0	0	0
Diseño	DI1	DI2	DI3	DI4	DI5
Factor Correctivo	0	0,25	0,25	0,5	1
Desarrollo	D1	D2	D3	D4	D5
Factor Correctivo	0	0,25	0,25	0,5	1
Pruebas	P1	P2	P3	P4	P5
Factor Correctivo	0	0,25	0,25	0,5	0,5
Otras tareas	T1	T2	T3	T4	T5
Factor Correctivo	0	0,25	0,25	0,5	1

Tabla 22. Factor correctivo en base al nivel de complejidad de la tarea

La estimación resultante para el proyecto es la indicada en la Figura 17, en la que se muestra el esfuerzo en horas y también se han incluido las jornadas equivalentes -los días-, resultado de dividir dicho esfuerzo entre ocho, que son las horas que tiene una jornada laboral normal.

Nombre del Proyecto											
GOBERNANZA CORPORATIVA DE LA TECNOLOGÍA DE LA INFORMACIÓN (T.I)											
		Jornadas Totales									
Actividad		Jornadas sin ponderar	Esfuerzo horas	Complejidad	Análisis	Diseño	Desarrollo	Otras actividades	Pruebas	Jornadas ponderadas	Esfuerzo horas ponderadas
Inicio		5	40							6,25	50
	Definición del alcance del proyecto.	1	8	T2				0,25		1,25	10
	Estimación del proyecto y de los recursos necesarios.	1	8	T2				0,25		1,25	10
	Elaboración de la propuesta de solución.	3	24	T3				0,25		3,75	30
Análisis		140	1120							140	1120
	Etapa de documentación	100	800	A2	0					100	800
	Definición de los elementos del cuestionario de autoevaluación.	40	320	A4	0					40	320
Diseño		65	520							110	880
	Definición de la arquitectura del entorno de desarrollo.	5	40	DI5		1				10	80
	Diseño de la solución propuesta.	20	160	DI5		1				40	320
	Definición de los modelos y cálculos para obtener los resultados de los cuestionarios.	20	160	DI5		1				40	320
	Elaboración de los cuestionarios.	20	160	DI4		0,5				20	160
Construcción		60	480							120	960
	Desarrollo del prototipo del cuestionario de autoevaluación.	60	480	D5			1			120	960
Pruebas Funcionales		10	80							12,5	100
	Realización de pruebas internas.	5	40	P2					0,25	6,25	50
	Corrección de errores detectados.	5	40	P2					0,25	6,25	50
Pruebas de Usuario		1	8							1	8
	Realización de pruebas finales.	1	8	P1					0	1	8
Implantación		7	56							7	56
	Presentación y entrega del proyecto.	7	56	T1				0		7	56
Memoria		100	800							125	1000
	Redacción de la memoria y tareas de revisión	100	800	T2				0,25		125	1000
TOTAL		388	3104							521,75	4174

Figura 17. Factor correctivo en base al nivel de complejidad de la tarea.

El siguiente paso es determinar los recursos necesarios y el coste unitario de los mismos. Se excluyen del presupuesto los costes ciertas tareas implícitas, como pueden ser los gastos luz, mantenimiento, etc.

Recursos Humanos	**€/Hora**	**Unidades**
Jefe de proyecto.	24	1
Analista.	15	1
Programador.	10	1
Testeador.	8	1
Documentador	8	1
Recursos Materiales	**Coste €**	**Unidades**
PC con Windows 8.1.	900	1
Cacoo.	0	1
Paquete Microsoft Office.	70	1
Adobe Acrobat Reader.	0	1
Gantter.	0	1
Eclipse.	0	1
JDK de Java.	0	1
Apache Tomcat.	0	1
My SQL.	0	1

Tabla 23. Tabla de recursos.

En base a esta información, se procede a elaborar la planificación del proyecto, representado mediante el diagrama Gantt correspondiente:

		Nombre	Duración	Inicio	Fin	Predecesoras	Recursos
0		⊟GOBERNANZA CORPORATIVA DE LA TECNOLOGÍA DE LA	343.25d?	01/09/2014	24/12/2015		

		Nombre	Duración	Inicio	Fin	Predecesoras	Recursos
1		ARRANQUE DEL PROYECTO.	0d?	01/09/2014	01/09/2014		
2		⊟**INICIO.**	**6.25d?**	**01/09/2014**	**09/09/2014**		
3		Definición del alcance del proyecto.	1.25d?	01/09/2014	02/09/2014		Jefe de proyecto
4		Estimación del proyecto y de los recursos necesarios.	1.25d?	02/09/2014	03/09/2014	3	Jefe de proyecto,Analista
5		Elaboración de la propuesta de solución.	3.75d?	03/09/2014	09/09/2014	4	Jefe de proyecto,Analista[50%]
6		FIN INICIO	0d?	09/09/2014	09/09/2014	5	
7		⊟**ANÁLISIS.**	**100d?**	**09/09/2014**	**27/01/2015**	**6**	
8		Etapa de documentación.	100d?	09/09/2014	27/01/2015		Analista[50%]
9		Definición de los elementos del cuestionario de autoevaluació	40d?	09/09/2014	04/11/2014		Analista[50%]
10		FIN ANÁLISIS.	0d?	27/01/2015	27/01/2015	8FF	
11		⊟**DISEÑO**	**110d?**	**27/01/2015**	**30/06/2015**	**10**	
12		Definición de la arquitectura del entorno de desarrollo.	10d?	27/01/2015	10/02/2015		Jefe de proyecto[50%],Analista
13		Diseño de la solución propuesta.	40d?	10/02/2015	07/04/2015	12	Jefe de proyecto[50%],Analista,Desarrollador[50%]
14		Definición de los modelos y cálculos para obtener los resulta	40d?	07/04/2015	02/06/2015	13	Jefe de proyecto[50%],Analista,Desarrollador[50%]
15		Elaboración de los cuestionarios.	20d?	02/06/2015	30/06/2015	14	Jefe de proyecto[50%],Analista,Desarrollador[50%]
16		FIN DISEÑO.	0d?	30/06/2015	30/06/2015	15FF	
17		⊟**CONSTRUCCIÓN.**	**120d?**	**30/06/2015**	**15/12/2015**	**16**	
18		Desarrollo del prototipo del cuestionario de autoevaluación.	120d?	30/06/2015	15/12/2015		Desarrollador[50%]
19		FIN CONSTRUCCIÓN.	0d?	09/07/2015	09/07/2015	26FF	
20		⊟**PRUEBAS FUNCIONALES.**	**6.25d?**	**30/06/2015**	**08/07/2015**	**17II**	
21		Realización de pruebas internas.	6.25d?	30/06/2015	08/07/2015		Testeador
22		Corrección de errores detectados.	6.25d?	30/06/2015	08/07/2015	21FF	Desarrollador[50%]
23		FIN PRUEBAS FUNCIONALES.	0d?	08/07/2015	08/07/2015	21FF,22FF	
24		⊟**PRUEBAS DE USUARIO.**	**1d?**	**08/07/2015**	**09/07/2015**	**20**	
25		Realización de pruebas finales.	1d?	08/07/2015	09/07/2015		Testeador
26		FIN PRUEBAS DE USUARIO.	1d?	08/07/2015	09/07/2015	25FF	
27		⊟**IMPLANTACIÓN.**	**7d?**	**15/12/2015**	**24/12/2015**	**31**	
28		Presentación y entrega del proyecto.	7d?	15/12/2015	24/12/2015		Jefe de proyecto
29		FIN IMPLANTACIÓN.	0d?	24/12/2015	24/12/2015	28FF	
30		REDACCIÓN DE LA MEMORIA	125d?	22/06/2015	15/12/2015	17FF	Documentador
31		FIN REDACCIÓN DE LA MEMORIA	1d?	14/12/2015	15/12/2015	19FF,30FF	
32		FIN PROYECTO.	0d?	24/12/2015	24/12/2015	29FF	
33		⊟**REVISIONES**	**290d?**	**01/09/2014**	**12/10/2015**		
34		Revisión 1.	0d?	01/09/2014	01/09/2014		Jefe de proyecto[50%]
35		Revisión 2.	0d?	17/09/2014	17/09/2014		Jefe de proyecto[50%]
36		Revisión 3.	0d?	23/12/2014	23/12/2014		Jefe de proyecto[50%]
37		Revisión 3.	0d?	13/02/2015	13/02/2015		Jefe de proyecto[50%]
38		Revisión 5.	0d?	06/04/2015	06/04/2015		Jefe de proyecto[50%]
39		Revisión 6.	0d?	14/05/2015	14/05/2015		Jefe de proyecto[50%]
40		Revisión 7.	0d?	08/06/2015	08/06/2015		Jefe de proyecto[50%]
41		Revisión 8.	0d?	03/07/2015	03/07/2015		Jefe de proyecto[50%]
42		Revisión 9.	0d?	29/07/2015	29/07/2015		Jefe de proyecto[50%]
43		Revisión 10.	0d?	26/08/2015	26/08/2015		Jefe de proyecto[50%]
44		Revisión 11.	0d?	14/09/2015	14/09/2015		Jefe de proyecto[50%]
45		Revisión 12.	0d?	22/09/2015	22/09/2015		Jefe de proyecto[50%]
46		Revisión 13.	0d?	12/10/2015	12/10/2015		Jefe de proyecto[50%]

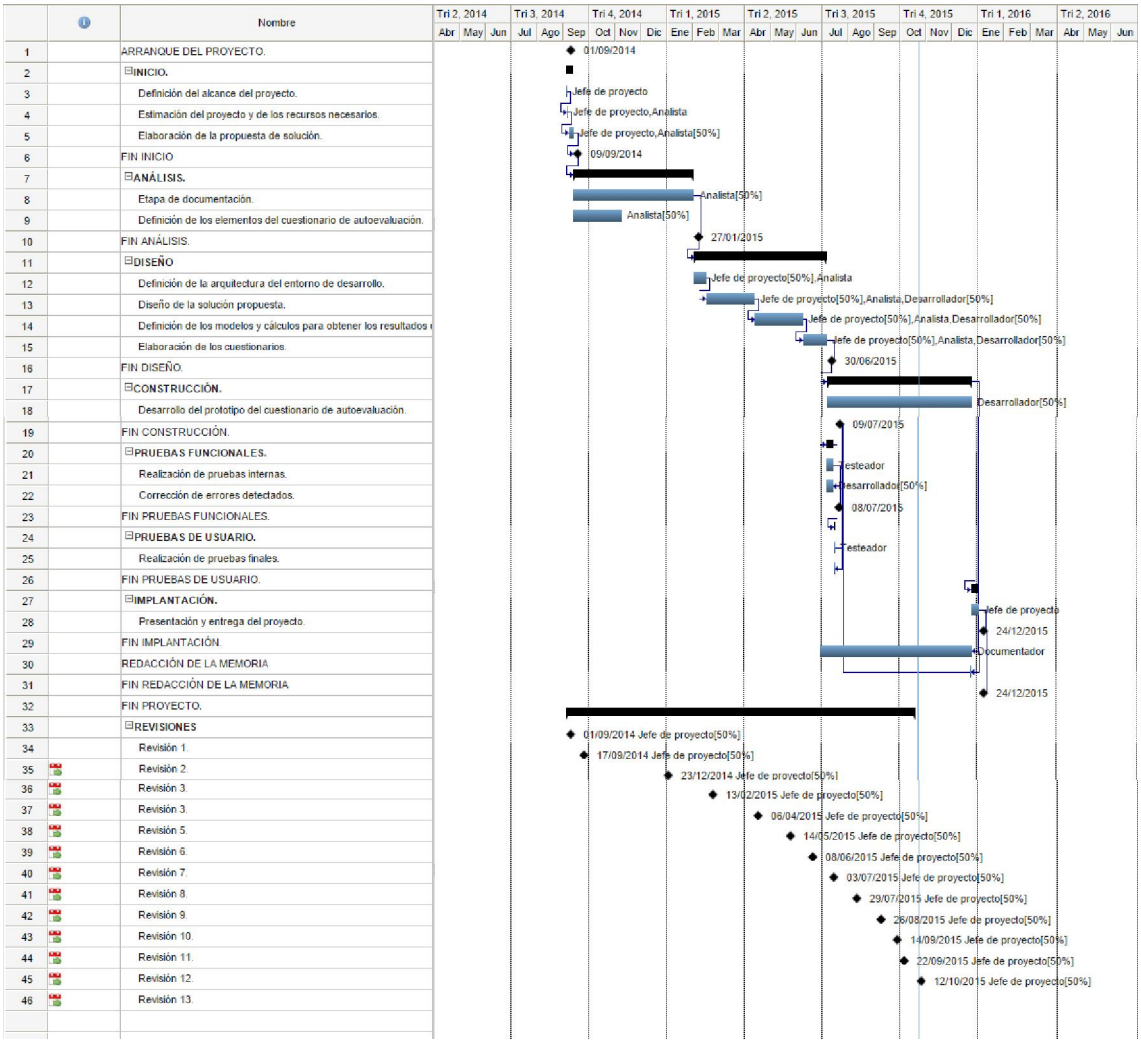

Figura 18. Diagrama Gantt.

El desglose del coste del proyecto en función de las tareas principales y de los recursos materiales necesarios sería por tanto el siguiente:

Tareas - Proyecto	**Coste €**
Inicio	**1575**
Definición del alcance del proyecto.	240
Estimación del proyecto y de los recursos necesarios.	390
Elaboración de la propuesta de solución.	945
Análisis	**8400**
Etapa de documentación.	6000
Definición de los elementos del cuestionario de autoevaluación.	2400
Diseño	**27760**
Definición de la arquitectura del entorno de desarrollo.	2160
Diseño de la solución propuesta.	10240
Definición de los modelos y cálculos para obtener los resultados de los cuestionarios.	10240
Elaboración de los cuestionarios.	5120
Construcción	**4800**
Desarrollo del prototipo del cuestionario de autoevaluación.	4800

Pruebas Funcionales	**650**
Realización de pruebas internas.	400
Corrección de errores detectados.	250
Pruebas de Usuario	**64**
Realización de pruebas finales.	64
Implantación	**1344**
Presentación y entrega del proyecto.	1344
Documentación	**8000**
Coste total Desarrollo del proyecto	**52593**
Recursos materiales.	**Coste €**
PC con Windows 8.1.	900
Cacoo.	0
Paquete Microsoft Office.	70
Adobe Acrobat Reader.	0
Gantter.	0
Eclipse.	0
JDK de Java.	0
Apache Tomcat.	0
My SQL.	0
Coste total Recursos materiales.	**970**
Coste total del proyecto	**53563**

Tabla 24. Desglose del presupuesto.

Por tanto, el presupuesto total del proyecto asciende a la cantidad de cincuenta y tres mil quinientos sesenta y tres Euros.

Capítulo 5
Conclusiones

Una vez finalizado el proyecto se analiza el resultado teniendo en cuenta los objetivos y las expectativas que se fijaron en un principio.

Por tanto, en este capítulo se anotan las conclusiones extraídas de la elaboración del proyecto y las líneas futuras que podrían realizarse sobre el mismo.

A lo largo del proyecto se ha comentado y destacado el papel estratégico de la Tecnología de la Información. Si hablamos de decisiones estratégicas, se debe escalar entonces la responsabilidad de toma de decisiones T.I a la Dirección de la empresa y este suele ser uno de los motivos de fracaso de los proyectos de este tipo: los miembros de la Dirección no tienen la formación suficiente, ni disponen del tiempo para profundizar en materia T.I, que les permita tomar las decisiones correctas. Además, las normas de buen gobierno corporativo sugieren que los miembros del Consejo sean independientes, lo que genera otro problema ya que no estos no conocen el negocio y, por tanto, tampoco las necesidades o los objetivos de la entidad.

En el panorama actual la mayoría de las empresas no contemplan la T.I como un activo más e incluso acaban delegando sus servicios y procesos a terceros (outsourcing). ¿La desventaja?, la empresa externa adquiere el conocimiento de los sistemas de información de la organización en la que están trabajando, de forma que, cuando entran a trabajar a otra empresa aplican estos conocimientos, eliminando así la ventaja competitiva de la primera entidad. Otro riesgo asociado es que la organización seguirá el ritmo que marque la empresa externa, que no tiene por qué ajustarse a las necesidades de la entidad.

La solución pasa por establecer los mecanismos necesarios que otorguen al Consejo la formación suficiente y necesaria que garantice la coherencia de sus decisiones T.I, y esto lo consigue la norma. Solamente si conocen las Tecnologías de la Información y la ventaja competitiva que aportan, pueden marcar la dirección y la forma de diferenciarse de la competencia.

A menor escala, este supuesto sería aplicable a los gestores o jefes de proyecto. Muchas veces, las personas asignadas a estos cargos ni siquiera tienen formación técnica y tampoco tienen la visión para aprovechar las tecnologías que maneja su equipo o comprender los problemas o dificultades que le trasladan. Siguiendo las indicaciones de la norma UNE-ISO/IEC 38500 estos puestos deberían ser ocupados por personas con las capacidades, habilidades y formación necesaria, por eso animo a inculcar a los estudiantes de las ingenierías que ese debe ser su cometido laboral, el de gestión de proyectos, incluso el de gobierno de las T.I, porque en el caso de la informática parece que nuestro trabajo está delegado al desarrollo de aplicaciones o programas.

Por tanto, en relación al uso e implantación de la norma UNE-ISO/IEC 38500 podemos concluir que:

- Asegura a las distintas partes interesadas (directores, clientes, inversores y empleados) que el seguimiento del estándar les va a permitir confiar en el gobierno corporativo de las Tecnologías de la Información: en la estrategia empresarial que definan, las inversiones realizadas, las decisiones que se tomen relacionadas con las T.I, etc.
- Sirve de guía a los directivos para el gobierno de las T.I.
- Constituye la base para poder evaluar de forma imparcial el estado del gobierno T.I en cualquier entidad, independientemente de su tamaño y sector al que se dedique.

Así que la norma es útil principalmente para dos colectivos:

- Dirección: indicándoles la forma en la que deben evaluar, dirigir y monitorizar las Tecnologías de la Información.
- Gestores T.I: les guía en las tareas de diseño e implementación de procesos y estructuras que den soporte al gobierno de las T.I.

Sobre la realización en sí del proyecto, aparte de conocer en detalle la norma UNE-ISO/IEC 38500, me ha permitido tener una visión general sobre los distintos marcos y normativas vigentes relacionadas. Del mismo, destacaría la elaboración del modelo de autoevaluación propuesto ya que, aunque existen recomendaciones sobre cómo implantar la norma, no detallan o especifican la forma de hacerlo y esto es lo que abarca nuestro modelo. Esta parte ha sido probablemente la más compleja y creo que el hecho de estar basado en marcos y modelos existentes, permitiría evaluar cualquier organización real y obtener unos resultados reales y objetivos.

Líneas futuras

A lo largo del proyecto se han incluido algunas mejoras que podrían realizarse como líneas futuras y que se resumen a continuación:

Realizar la evaluación de todos los procesos COBIT, no sólo los procesos del marco que soportan la norma UNE-ISO/IEC 38500, de esta manera con un mismo modelo conseguimos evaluar el nivel de capacidad de la organización siguiendo el marco COBIT5 y obtener el nivel de madurez de cada uno de los principios del estándar.

De manera general, para los diferentes cuestionarios podría incluirse un peso, por ejemplo, de 0 a 5 o de 0 a 10, de forma que el usuario en base a ese valor determinara la importancia en su organización de cada pregunta que conforma el cuestionario. El nivel resultante de cada proceso se calcularía teniendo en cuenta el peso asignado por el usuario y el grado de cumplimento de cada pregunta.

En relación al diseño de la aplicación propuesta:

Si en algún momento se manejara un volumen elevado de datos otra opción de mejora sería integrar la aplicación con algún módulo de desarrollo de Big Data, por ejemplo, Apache Hadoop, o con alguna herramienta de Business Intelligence (B.I), como puede ser QlikView que cuenta con una opción de descarga gratuita. Para futuras versiones también podría plantearse desarrollar la aplicación Java utilizando el marco de trabajo JSF y la librería ICEfaces pues, además de facilitar y simplificar el desarrollo, permiten el funcionamiento correcto de la aplicación en distintos sistemas operativos sin necesidad de modificar el código fuente.

Completar la funcionalidad permitiendo al auditor externo comparar más de dos organizaciones. También podrían añadirse gráficos para contrastar los resultados.

Ampliar los campos correspondientes a la organización, para poder incluir las divisiones territoriales de otros países.

Todas las operaciones que ahora mismo están contempladas dentro de la lógica de desarrollo de la aplicación y que se han definido para establecer los cálculos de los cuestionarios, podrían estar visibles, dando a conocer al usuario estos valores y los cálculos intermedios.

Por último, aunque no estaba dentro del alance del proyecto, se ha desarrollado un prototipo que soporte el modelo de autoevaluación propuesto. Esta aplicación, aunque tiene definido e implementado el modelo de base datos, las páginas correspondientes y estructura principal de clases, no tiene desarrollada toda la lógica de negocio. Podría en versiones futuras completarse la funcionalidad, incluso ampliarla desarrollando una aplicación que contemplara además todos los pasos necesarios para la implantación de gobierno T.I en una entidad, para la cual podría utilizarse como guía orientativa este proyecto.

Glosario

Acrónimos y siglas

AENOR	- Asociación Española de Normalización y Certificación.
ANSI	- American National Standards Institute. - Instituto Nacional Estadounidense de Estándares.
APO	- Align, Plan and Organise. - Alinear, Planificar y Organizar.
BAI	- Build, Acquire and Implement. - Construir, Adquirir e Implementar.
B.I	- Business Intelligence. - Inteligencia Empresarial.
BSI	- British Standards Institution. - Instituto Británico de Normalización.
CMMi	- Capacity Madurity Model Integrated. - Integración de Modelos de Madurez de Capacidades.
COBIT	- Control Objectives for Information and related Technology. - Control de Objetivos para la Información y Tecnología relacionada.
COSO	- Committee of Sponsoring Organizations of the Treadway Commission. - Comité de Organizaciones Patrocinadoras de la Comisión Treadway.
CRM	- Customer Relationship Management. - Gestión de Relaciones con el Cliente.
DoDAF	- Department of Defense Architecture Framework. - Marco de Arquitectura del Departamento de Defensa.
DSS	- Deliver, Service and Support. - Entregar, dar Servicio y Soporte.
EDM	- Evaluate, Direct and Monitor. - Evaluar, Dirigir y Monitorizar.

FEAF	- Federal Enterprise Architecture Framework. - Marco de Arquitectura Empresarial Federal.
IEC	- Comisión Electrotécnica Internacional.
IEEE	- Institute of Electrical and Electronics Engineers. - Instituto de Ingeniería Eléctrica y Electrónica.
ISACA	- Information Systems Audit and Control Association. - Asociación de Auditoría y Control de Sistemas de Información.
ITIG	- IT Governance Institute. - Instituto de Gobierno T.I.
ITIL	- IT Infraestructure Library. - Biblioteca de Infraestructura de Tecnologías de Información.
JDK	- Java Development Kit. - Kit de Desarrollo Java.
JSF	- JavaServer Faces. - Marco de trabajo de interfaces de usuario del lado de servidor para aplicaciones Web basadas en tecnología Java.
MEA	- Monitor, Evaluate and Assess. - Supervisar, Evaluar y Valorar.
PDF	- Portable Document Format. - Formato de Documento Portátil.
PEMM	- Process and Enterprise Maturity Model. - Modelo de Madurez de Proceso y de Empresa.
PDCA	- Plan, Do, Check, Act. - Planificar, Hacer, Construir y Actuar.
PMBoK	- Project Management Body of Knowledge. - Fundamentos para la Dirección de Proyectos.
PRINCE2	- Projects in Controlled Environments. - Proyectos en Ambientes Controlados.
ROI	- Return on Investment - Retorno de Inversión.
SAM	- Software Asset Managament. - Gestión de Activos Software.

SGCN	- Sistema de Gestión de la Continuidad del Negocio.
SGSI	- Sistemas de Gestión de la Seguridad de la Información.
SGSTI	- Sistemas de Gestión de Servicios de T.I.
S.I	- Sistemas de Información.
SLA	- Service Level Agreement. - Acuerdo de Nivel de Servicio.
SPICE	- Software Process Improvement and Capability Determination. - Determinación de la Capacidad de Mejora del Proceso de Software.
SQuaRE	- Software product Quality Requirements and Evaluation. - Requisitos de Calidad y Evaluación de Productos de Software.
T.I	- Tecnología de la Información.
TIC	- Tecnología de la Información y Comunicaciones.
TOGAF	- The Open Group Architecture Framework. - Esquema de Arquitectura del Open Group.
VSE	- Very Small Entity. - Entidades Muy Pequeñas.

Anotaciones

[g] AENOR. Es la Asociación Española de Normalización y Certificación, que se dedica a la elaboración de normas nacionales, a la certificación de productos, entidades, etc. También ofrece orientación a aquellas entidades que quieran certificarse. **[55]**

Mencionar también el **ANSI,** el Instituto Nacional Estadounidense de Estándares, las siglas provienen del inglés American National Standards Institute. Esta organización tiene un carácter internacional y se ocupa del desarrollo y supervisión de estándares relacionados con los sistemas, procesos, productos y servicios. **[73] [74]**

[e] Arquitectura empresarial. Describe los elementos que componen una organización y las relaciones de estos elementos. Su finalidad es optimizar los procesos de la entidad para que se puedan alcanzar los objetivos de negocio y la empresa pueda responder de forma adecuado a los cambios. **[49]**

[b] COSO. El acrónimo viene del inglés, Committee of Sponsoring Organizations of the Treadway Commission, que se puede traducir como Comité de Organizaciones Patrocinadoras de la Comisión Treadway. Es una entidad privada, cuyo objetivo es orientar a las empresas en temas de gestión y gobierno. COSO define un modelo que pueden utilizar las organizaciones para evaluar sus sistemas de control interno. **[75]**

[h] El ciclo PDCA. Corresponde a las tareas de Planificar, Hacer, Verificar y Actuar (Plan, Do, Check, Act), presentes en cualquier actividad de mejora continua y en los procesos de gestión de servicios T.I. A modo de resumen **[76]**:

- Planificar: en esta fase se definen los objetivos y los recursos necesarios para lograrlos.
- Hacer: se llevan a cabo las tareas de implementación de los procesos diseñados, controles, etc.
- Verificar: se evalúa si se han alcanzado las metas definidas.
- Actuar: se analizan las desviaciones respecto a lo planificado o establecido, y se proponen medidas para corregirlas y mejorar los procesos empleados.

[d] ISACA. Son las siglas de Information Systems Audit and Control Association, Asociación de Auditoría y Control de Sistemas de Información. ISACA es una entidad internacional que defiende y promueve el uso de certificaciones y metodologías en las auditorías y en las actividades de control. **[77]**

[c] ITGI. Instituto de Gobierno TI (IT Governance Institute). Es una asociación fundada por ISACA pero de carácter independiente, que proporciona investigaciones, publicaciones y recursos sobre la gobernanza de T.I. **[78]**

[f] JTC 1. Es una comisión técnica creada conjuntamente entre ISO y la IEC (Comisión Electrotécnica Internacional). JTC 1 desarrolla las normas y estándares relacionados con la Tecnología de la Información, requeridos por los mercados globales para satisfacer los requisitos de negocio y usuarios, entre otros, en temas de diseño y desarrollo de sistemas y herramientas T.I, seguridad y calidad de las T.I. **[79]**

[a] Modelo de negocio. El modelo de negocio se refiere a la concepción de cómo una empresa hace negocio y genera ingresos. **[69]**

[i] Nomenclatura de las normas:

Los estándares ISO se designan utilizando el siguiente formato:

ISO [/IEC] [/ASTM] [IS] número [-p]:[yyyy] Título

- *IEC,* se incluye si el estándar es el resultado del trabajo del ISO/IEC y el JTC1.
- *ASTM* (American Society for Testing and Materials) se usa para estándares desarrollados en cooperación con el ASTM International.
- *IS,* si es un estándar internacional.
- *número* es el número del estándar.
- *p* es una parte numérica opcional.
- *yyyy* es el año de publicación.
- *Título* describe el nombre o asunto de la norma.

Existen otras abreviaciones complementarias que determinan el estado de la norma y las enmiendas.

Las normas UNE: las siglas corresponden Una Norma Española. Se trata del nombre que reciben las normas elaboradas por AENOR. Se nombran siguiendo la siguiente nomenclatura:

Norma	A	B	C
UNE	1	'032	82

A: representa al comité al que pertenece la norma.

B: número de la norma. Puede ir acompañado de una R, si se trata de una revisión; M, para modificaciones o C, para los complementos.

C: indica el año de edición de la norma.

Normas EN: Son normas europeas, que se llevan a cabo bajo siguiendo las directrices del CEN (Comité Europeo de Normalización) y que posteriormente, tras ser validadas, se editan como normas EN.

Normas UNE EN: son aquellas normas europeas, adaptadas a su versión en español, que son aceptadas y adoptadas dentro de AENOR. **[80] [81]**

Referencias

Las referencias en orden de aparición de la memoria son:

[1] Las herramientas de gestión del conocimiento. Una visión integrada.
Disponible [Internet]:
<http://www.adingor.es/Documentacion/CIO/cio2004/comunicaciones/725-734.pdf>
[Accedido el 14 de Septiembre de 2014].

[2] InformeTICfacil.com.
Disponible [Internet]:
<http://www.informeticplus.com/que-son-las-tecnologias-de-la-informacion>
[Accedido el 14 de Septiembre de 2014].

[3] tics.
Disponible [Internet]:
< http://uagro104vespertino.blogspot.com.es/2015/01/concepto-de-tegnologias-de-la.html >
[Accedido el 14 de Septiembre de 2014].

[4] Andreu, R., Ricart J.E. y Valor, J.: "Estrategia y Sistemas de información". (Mc Graw-Hill, Madrid, 1991).

[5] Cohen, D., Asín, E.: "Sistemas de información para los negocios: un enfoque para la toma de decisiones". (Mc Graw-Hill, México, 2005).

[6] monografías.com > Sistema de Información.
Disponible [Internet]:
<http://www.monografias.com/trabajos7/sisinf/sisinf.shtml>
[Accedido el 14 de Septiembre de 2014].

[7] Pavez, A.: "Modelo de implantación de Gestión del Conocimiento y Tecnologías de Información para la Generación de Ventajas Competitivas". Valparaíso: Universidad Técnica Federico Santa María, 2000.

[8] Aumatell, C.: "Auditoría de la información. Identificar y explotar la información en las organizaciones". (UOC, Barcelona, 2012).

[9] Sáez Vacas, F. "Las tecnologías de la tercera revolución de la información", Mundo electrónico, núm. 183, pág. 133- 141. (1983).

[10] Valle, R., Ros, F., Barberá, J. y Gamella, M.: "Tecnologías de la información: electrónica, informática y telecomunicaciones", Notas del curso "Fundamentos y función de la ingeniería", ETSI Telecomunicación, Madrid (tomado del libro "Los países industrializados ante las nuevas tecnologías", FUNDESCO). (1986).

[11] Álvarez, Antonio. "Influencia de las tecnologías de la información en los procesos de información y toma de decisiones de las empresas". Primer Congreso Universitario de Ciencias de la Documentación, Madrid, España, 2000.

[12] Lucas, H. C.: "Implementation the Key to Successful Information Systems". (Columbia University Press, New York, 1981).

[**13**] El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento.
Disponible [Internet]:
<http://www.ehu.eus/zer/hemeroteca/pdfs/zer27-14-cobo.pdf>
[Accedido el 3 de Octubre de 2014]

[14] Sistemas de la información estratégicos y tecnologías de la información.
Disponible [Internet]:
<sistemas_de_informacion_estrategicos_y_tecnologias_de_la_inf.pdf>
[Accedido el 3 de Octubre de 2014].

[15] Revilla, E.: "Reflexiones en torno al valor estratégico de la tecnología de la información". Anales de Estudios de Economía y Empresa, núm. 6, pág. 67-81. (1991).

[16] Calder, A., y Moir, S.: "IT Governance. Implementing Frameworks and Standards for the Corporate Governance of IT". (IT Governance Publishing, UK, 2009).

[17] Garzas, J., Fernández, C.M. y Piattini, M.: "Una aplicación de ISO/IEC 15504 para la evaluación por niveles de madurez de PYMEs y pequeños equipos de desarrollo", Revista Española de Innovación, Calidad e Ingeniería del Software," núm. 2, volumen 5, pág. 88-98 (2009).

[18] MCFARLAN, F.: "La tecnología de la información cambia el modo de competir". Harvard Deusto Business Review, 2º trimestre, pág. 43-50. (1985).

[19] Blog > Blog PUCP.
Disponible [Internet]:
< blog.pucp.edu.pe >
[Accedido el 22 de Octubre de 2014].

[20] Blog > Las Tecnologías de Información en la Organización.
Disponible [Internet]:
< http://marcodegobdelasti.blogspot.com.es/>
[Accedido el 22 de Octubre de 2014].

[21] Throp, J.: "Monografía Gobierno corporativo de las TI", Novática, núm. 229, pág. 48-55. (Julio - Septiembre 2014).

[22] Definición del proceso de auditoría interna del aspecto adquisición, desarrollo y mantenimiento de sistemas de información para gestión de seguridad de la información soportado en TICs.
Disponible [Internet]:
<repositorio.utp.edu.co/dspace/bitstream/11059/4119/1/0058M491D.pdf>
[Accedido el 26 de Octubre de 2014].

[23] Toomey, M.: "Waltzing with the Elephant: A comprehensive guide to directing and controlling information technology". (Infonomics, Australia, 2009).

[24] Presentación - Tema 2 - Introducción a la auditoría de sistemas de información.
Disponible [Internet]:
<http://www.dcc.etsii.urjc.es/sites/default/files/Presentacion - Tema 2 - Introduccion a la auditoria de sistemas de informacion.pdf>
[Accedido el 28 de Octubre de 2014].

[25] Control Interno.
Disponible [Internet]:
<http://veronicavafi.jimdo.com/app/download/7140526268/CONTROL%2BINTERNO.pdf?t=1358974842.>
[Accedido el 28 de Octubre de 2014].

[26] Piattini, M., del Peso, E.; del Peso, M.: "Auditoría de tecnologías y sistemas de información". (Ra-Ma, Madrid, 2008).

[27] wordpress > Control Interno Informático.
Disponible [Internet]:
<https://noris14.wordpress.com/2011/06/10/control-interno-informatico/>
[Accedido el 3 de Noviembre de 2014].

[28] Ramos, M.A: "Auditoría Informática". (Universidad Carlos III de Madrid. E.P.S Informática, 2004).

[29] Control interno y auditoría informática**.**
Disponible [Internet]:
<es.slideshare.net/RobertoPorozo/control-interno-y-auditoria-informtica>
[Accedido el 18 de Noviembre de 2014].

[30] Principios de Gobierno Corporativo de la OCDE, Organización para la Cooperación y el Desarrollo Económicos, 2004.
Disponible [Internet]:
<http://www.oecd.org/daf/ca/corporategovernanceprinciples/37191543.pdf>
[Accedido el 30 de Noviembre de 2014].

[31] La Contribución del Balanced Scorecard al Proceso de Gobierno de Tecnología de Información (TI).
Disponible [Internet]:
<http://www.ucema.edu.ar/posgrado-download/tesinas2001/Rizzo-MADE.pdf>
[Accedido el 30 de Noviembre de 2014].

[32] Confecámaras > Qué es gobierno corporativo.
Disponible [Internet]:
<http://www.confecamaras.org.co/gobierno-corporativo/165-que-es-gobierno-corporativo>
[Accedido el 6 de Diciembre de 2014].

[33] Fernández, C., Piattini, M.: "Modelo para el gobierno de las TIC basado en las normas ISO". (AENORediciones, Madrid, 2012).

[34] Santiago, D.: "Análisis y Estudio sobre el Gobierno y Gestión de los Servicios TI en el mercado español". Universidad Carlos III de Madrid, 2010.

[35] Barger, Teresa. "Corporate Governance – A Working Definition". IFC/OECD INTERNATIONAL CORPORATE GOVERNANCE MEETING, Hanoi, Vietnam, 2004.

[36] Fernández, A.: "ANÁLISIS, PLANIFICACIÓN Y GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LAS UNIVERSIDADES". Universidad de Almería, 2009.

[37] Muñoz, I; Ulloa, G.: "Gobierno de TI". Revista S&T, núm. 9(17), pág. 23-53 (2011).

[38] Rizzo, Mª E.: "La Contribución del Balanced Scorecard al Proceso de Gobierno de Tecnología de Información (TI)". Universidad del CEMA, 2001.

[39] ISO/IEC 20000.Guía completa de aplicación para la gestión de los servicios de tecnologías de la información.
Disponible [Internet]:
<PUB_DOC_Tabla_AEN_7172_1.pdf**>**
[Accedido el 12 de Diciembre de 2014].

[40] Blogspot > Fundamentos de Gestión de Servicios T.I.
Disponible [Internet]:
<http://fundamentosdegestiondeserviciosdeti.blogspot.com.es/>
[Accedido 12 de Diciembre de 2014].

[41] tcp > Gobierno IT.
Disponible [Internet]:
<http://www.tcpsi.com/servicios/gobierno_ti.htm>
[Accedido 12 de Diciembre de 2014].

[42] Universidad de Cuenca > Auditoría Informática.
Disponible [Internet]:
<http://dspace.ucuenca.edu.ec/bitstream/123456789/652/3/ts205.pdf.txt>
[Accedido 14 de Enero de 2015].

[43] Wiki.es > Procesos ITIL.
Disponible [Internet]:
<http://wiki.es.it-processmaps.com/index.php/Procesos_ITIL>
[Accedido 27 de Enero de 2015].

[44] Wikipedia > Project Management Institute.
Disponible [Internet]:
<https://es.wikipedia.org/wiki/Project_Management_Institute>
[Accedido el 27 de Enero de 2015].

[45] PMBOK.
Disponible [Internet]:
<http://temasselectossw.galeon.com/productos1835364.html>
[Accedido el 13 de Febrero de 2015].

[46] QRP Internacional > ¿Qué es PRINCE2?
Disponible [Internet]:
<http://www.qrpinternational.es/index/prince-2/what-is-prince2>
[Accedido el 1 Marzo de 2015].

[47] CMMI Institute.
Disponible [Internet]:
<http://cmmiinstitute.com/about-cmmi-institute>
[Accedido el 16 de Marzo 2015].

[48] Val IT 2.0 – Valor Empresario: Gobierno de las Inversiones en TI.
Disponible [Internet]:
<http://cafrancavilla.com/2009/08/08/val-it-2-0-valor-empresario-gobierno-de-las-inversiones-en-ti/>
[Accedido el 3 Mayo 2015].

[49] Cintel > ARQUITECTURA EMPRESARIAL: UN NUEVO RETO PARA LAS EMPRESAS DE HOY.
Disponible [Internet]:
<http://cintel.org.co/wp-content/uploads/2013/05/04.SOA_-_Eva_Maya.pdf>
[Accedido el 3 Mayo 2015].

[50] TOGAF Versión 9.1.
Disponible [Internet]:
<http://www.vanharen.net/Samplefiles/9789087537104SMPL.pdf>
[Accedido el 11 Mayo 2015].

[51] Wikipedia > TOGAF.
Disponible [Internet]:
<https://es.wikipedia.org/wiki/TOGAF>
[Accedido el 11 Mayo 2015].

[52] Arquitectura Empresarial en acción > Motivación de Zachman.
Disponible [Internet]:
<https://arquitecturaempresarialcali.wordpress.com/ensayos/motivacion-de-zachman/>
[Accedido el 11 de Junio de 2015].

[53] Lucio, T.:" Marco para la definición y adecuación de una service management office en el contexto de los servicios de tecnologías de la información". Universidad Carlos III de Madrid, 2013.

[54] Isaca > Gobierno de las TIC ISO/IEC 38500.
Disponible [Internet]:
<http://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Gobierno-de-las-TIC-ISO-IEC-385001.aspx>
[Accedido el 11 de Junio de 2015].

[55] AENOR > UNE-EN ISO 22301:2015.
Disponible [Internet]:
<http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0054336&pdf=#.VX_WFFLtmYw>
[Accedido el 14 de junio de 2015].

[56] ISOTools > ISO 27001: Las TIC, más seguras que nunca. [↑]
Disponible [Internet]:
<https://www.isotools.org/2014/11/25/iso-27001-tic-mas-seguras-que-nunca/#sthash.xDGNDQMe.dpbs>
[Accedido el 14 de Junio de 2015].

[57] Procesos Software ISO 15504:2004.
Disponible [Internet]:
<http://procesosoftwareai.blogspot.com.es/2012/10/isoiec-155042004.html>
[Accedido el 29 de Mayo 2015].

[58] ISO > ISO 12207:2008.
Disponible [Internet]:
<http://www.iso.org/iso/catalogue_detail?csnumber=43447>
[Accedido el 29 Mayo 2015].

[59] AENOR.
Disponible [Internet]:
<http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0041542#.VgPAgX0pr8k>
[Accedido el 14 de Junio de 2015].

[60] ISO > ISO/IEC TR 29110-1:2011.
Disponible [Internet]:
<http://www.iso.org/iso/catalogue_detail?csnumber=51150>
[Accedido el 29 de Mayo 2015].

[61] ISO > ISO/IEC 25000: 2005.
Disponible [Internet]:
<http://www.iso.org/iso/catalogue_detail.htm?csnumber=35683>
[Accedido el 29 de Mayo 2015].

[62] Wikipedia > ISO/IEC 25000.
Disponible [Internet]:
<http://es.wikipedia.org/wiki/ISO/IEC_25000>
[Accedido el 29 de Mayo 2015].

[63] ISO > ISO/IEC 25000:2014.
Disponible [Internet]:
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64764
>
[Accedido el 14 de Junio de 2015].

[64] Javier Garzas > ISO/IEC 29119.
Disponible [Internet]:
<http://www.javiergarzas.com/2009/03/isoiec-29119-hacia-un-nueva-norma-para.html>
[Accedido el 29 de Mayo 2015].

[65] Gobierno de las TI para las universidades.
Disponible [Internet]:
<http://www.crue.org/Publicaciones/Documents/Gobierno%20TI/gobierno
de_las_TI_para_universidades.pdf>
[Accedido 14 de Diciembre de 2014].

[**66**] ITIG: "ITGI Facilita la Adopción de IS0/IEC 38500:2008". (IT Governance Institute, EEUU, 2009)

[67] IT Governance: Cobit 5.
Disponible [Internet]:
<https://articulosit.files.wordpress.com/2013/07/it-governance-cobit-5.pdf>
[Accedido el 11 de Agosto 2015].

[68] ISO/IEC TR, Tecnología de la información – Proceso de evaluación - Parte 7: Evaluación de la madurez de la organización, ISO/IEC TR 15504-7:2008.

[69] Hammer >Process and Enterprise Maturity Model - (PEMM).
Disponible [Internet]:
<http://www.hammerandco.com/HammerAndCompany.aspx?id=58>
[Accedido el 5 de Agosto 2015].

[70] Pino, F.J.; Piattini, M., Fernández, C.M.: "Modelo de madurez de ingeniería del software"). (AENORediciones, Madrid, 2014).

[71] Cuaderno ISACA.
Disponible [Internet]:
<8-20710-05-06_ISACAMadrid - Cuaderno 0001_GBA_v01.00.pdf>
[Accedido el 22 de Abril 2015].

[72] Universitat Overta de Catalunya> Enfoque Comercial de la Fase de Definición de un Proyecto Informático.
Disponible [Internet]:
<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/891/1/34954tfc.pdf>
[Accedido el 6 de Septiembre 2015].

[73] ANSI.
Disponible [Internet]:
<http://www.ansi.org/>
[Accedido el 19 de Abril de 2015].

[74] Wikipedia > Instituto Nacional Estadounidense de Estándares.
Disponible [Internet]:
<http://es.wikipedia.org/wiki/Instituto_Nacional_Estadounidense_de_Est%C3%A1ndares>
[Accedido el 19 de Abril de 2015].

[75] COSO.
Disponible [Internet]:
<www.**coso**.org>
[Accedido el 19 de Abril de 2015].

[76] ITIL Foundation - Gestión de servicios > Ciclo Deming.
Disponible [Internet]:
<http://itilv3.osiatis.es/proceso_mejora_continua_servicios_TI/ciclo_deming.php>
[Accedido el 19 de Abril de 2015].

[77] ISACA.
Disponible [Internet]:
<https://www.isaca.org/>
[Accedido el 19 de Abril de 2015].

[78] ITIG.
Disponible [Internet]:
<http://www.itgi.org/>
[Accedido el 23 de Abril de 2015].

[79] ISO/IEC JTC 1.
Disponible [Internet]:
<http://www.iso.org/iso/jtc1_home.html>
[Accedido el 23 de Abril de 2015].

[80] Blog Asesor de Calidad >QUÉ SIGNIFICAN LAS SIGLAS: UNE, EN, ISO Y CTN.
Disponible [Internet]:
<http://asesordecalidad.blogspot.com/2014/10/que-significan-las-siglas-une-en-iso-y.html#.VXIJAlLtmYw>
[Accedido el 27 de Abril de 2015].

[81] Wikipedia > Norma UNE.
Disponible [Internet]:
<http://es.wikipedia.org/wiki/Norma_UNE>
[Accedido el 27 de Abril de 2015].

[82] Blog > IT – Governance, Risk & Compliance.
Disponible [Internet]:
<https://francoitgrc.wordpress.com/2012/04/14/cobit-5-update-por-version-oficial-de-isaca/>
[Accedido el 27 de Septiembre de 2015]

Bibliografía

Libros

Andreu, R., Ricart J.E. y Valor, J.: "Estrategia y Sistemas de información". (Mc Graw-Hill, Madrid, 1991).

Aumatell, C.: "Auditoría de la información. Identificar y explotar la información en las organizaciones". (UOC, Barcelona, 2012).

Calder, A., y Moir, S.: "IT Governance. Implementing Frameworks and standards for the Corporate Governance of IT". (IT Governance Publishing, UK, 2009).

Calder, A., y Watkins, S.: "IT Governance. A Manager's Guide to Data Security and ISO 27001/ISO27002". (Kogan Page Limited, UK, 2008).

Cohen, D., Asín, E.: "Sistemas de información para los negocios: un enfoque para la toma de decisiones". (Mc Graw-Hill, México, 2005).

Dagoberto, J.: "Auditoría informática: aplicaciones en producción". (Ecoe Ediciones, Bogotá, 1997).

Fernández, C., Piattini, M.: "Modelo para el gobierno de las TIC basado en las normas ISO". (AENORediciones, Madrid, 2012).

Galliers, D., Leidner, D.: "Strategic Information Management. Challenges and strategies in managing information systems". (Butterworth-Heinemann, Oxford, 2003).

ITIG: "ITGI Facilita la Adopción de IS0/IEC 38500:2008". (IT Governance Institute, EEUU, 2009)

[Lucas, H. C.: "Implementation the Key to Successful Information Systems". (Columbia University Press, New York, 1981).

Piattini, M., del Peso, E.; del Peso, M.: "Auditoría de tecnologías y sistemas de información". (Ra-Ma, Madrid, 2008).

Pino, F.J.; Piattini, M., Fernández, C.M.: "Modelo de madurez de ingeniería del software"). (AENORediciones, Madrid, 2014).

Ramos, M.A: "Auditoría Informática". (Universidad Carlos III de Madrid. E.P.S Informática, 2004).

Toomey, M.: “Waltzing with the Elephant: A comprehensive guide to directing and controlling information technology”. (Infonomics, Australia, 2009).

Whittington, O., Pany, K.: “Principios de auditoría”. (Mc Graw-Hill, México, 2005).

Revistas

Andrade, J.: “Tecnologías y sistemas de información en la gestión de conocimiento en las organizaciones”, Revista Venezolana de Gerencia, núm. 24, volumen 8, pág. 558-574. (2003).

Garzas, J., Fernández, C.M. y Piattini, M.: “Una aplicación de ISO/IEC 15504 para la evaluación por niveles de madurez de PYMEs y pequeños equipos de desarrollo”, Revista Española de Innovación, Calidad e Ingeniería del Software,” núm. 2, volumen 5, pág. 88-98 (2009).

MCFarlan, F.: “La tecnología de la información cambia el modo de competir”. Harvard Deusto Business Review, 2º trimestre, pág. 43-50. (1985).

Muñoz, I; Ulloa, G.: “Gobierno de TI”. Revista S&T, núm. 9(17), pág. 23-53 (2011).

Revilla, E.: “Reflexiones en torno al valor estratégico de la tecnología de la información”. Anales de Estudios de Economía y Empresa, núm. 6, pág. 67-81. (1991).

Sáez Vacas, F. "Las tecnologías de la tercera revolución de la información", Mundo electrónico, núm. 183, pág. 133- 141. (1983).

Throp, J.: “Monografía Gobierno corporativo de las TI”, Novática, núm. 229, pág. 48-55. (Julio-Septiembre 2014).

Valle, R., Ros, F., Barberá, J. y Gamella, M.: "Tecnologías de la información: electrónica, informática y telecomunicaciones", Notas del curso "Fundamentos y función de la ingeniería", ETSI Telecomunicación, Madrid (tomado del libro “Los países industrializados ante las nuevas tecnologías”, FUNDESCO). (1986).

Congresos o reuniones

Álvarez, Antonio. "Influencia de las tecnologías de la información en los procesos de información y toma de decisiones de las empresas". Primer Congreso Universitario de Ciencias de la Documentación, Madrid, España, 2000.

Barger, Teresa. "Corporate Governance – A Working Definition". IFC/OECD INTERNATIONAL CORPORATE GOVERNANCE MEETING, Hanoi, Vietnam, 2004.

Normas, marcos y estándares

AENOR, Gobernanza corporativa de la Tecnología de la Información (TI), UNE-ISO/IEC 38500:2013.

COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.

ISO, Determinación de la Capacidad de Mejora del Proceso de Software, SPICE ISO 15504:2004.

ISO, Sistemas e ingeniería de software - procesos de ciclo de vida de Software, ISO 12207:2008.

ISO/IEC, Ingeniería Software – Perfiles de ciclo de vida para Entidades Muy Pequeñas, ISO/IEC 29110:2011.

ISO/IEC, Modelo de evaluación, mejora y madurez del software, ISO/IEC 15504.

ISO/IEC, Pruebas de Software, ISO/IEC 29119:2013.

ISO/IEC, Sistemas e Ingeniería de Software - Requisitos de Calidad y Evaluación de Productos de Software (SQuaRE) - Guía de SquaRE, ISO/IEC 25000:2014.

ISO/IEC TR, Tecnología de la Información – Proceso de evaluación - Parte 7: Evaluación de la madurez de la organización, ISO/IEC TR 15504-7:2008.

UNE, Gestión de la continuidad del negocio, UNE 71599-2:2010.

UNE-EN ISO, Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012), UNE-EN ISO 22301:2015.

UNE-ISO/IEC, Tecnología de la Información. Gestión de activos de software (SAM). Parte 1: Procesos, UNE-ISO/IEC 19770-1:2008.

UNE-ISO/IEC, Tecnología de la Información. Gestión del servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio, UNE-ISO/IEC 20000-1:2011.

UNE-ISO/IEC, Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos, UNE-ISO/IEC 27001:2014.

Páginas o documentos electrónicos en la red

12manage > Metodología PMBOK.
<http://www.12manage.com/methods_pmi_pmbok_es.html>
[Accedido el 11 de Junio 2015].

ACIS > Análisis y control de riesgos de seguridad informática: control adaptativo.
<http://www.acis.org.co/fileadmin/Revista_105/JMGarcia.pdf>
[Accedido el 17 de Noviembre 2014].

Aemes TI > Gobernanza TI y el estándar ISO 38500.
<http://www.aemes.org/index.php/historico-de-noticias/1-ultimas-noticias/75-gobernanza-ti-y-el-estandar-iso-38500>
[Accedido el 13 de Ocutbre 2014].

AENOR.
<http://www.aenor.es/aenor/inicio/home/home.asp>
[Accedido el 14 de Junio de 2015].

AENOR > UNE-EN ISO 22301:2015.
<http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0054336&pdf=#.VX_WFFLtmYw>
[Accedido el 16 de junio de 2015].

AENOR> UNE-ISO/IEC 27001:2014.
<http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0053761#.VX3EcVLtmYw>
[Accedido el 14 de Junio de 2015].

ANSI.
<http://www.ansi.org/>
[Accedido el 19 de Abril de 2015].

Arquitectura Empresarial en acción > Motivación de Zachman.
<https://arquitecturaempresarialcali.wordpress.com/ensayos/motivacion-de-zachman/>
[Accedido el 11 de junio de 2015].

ArticuloZ > La Importancia De La Auditoría De La Calidad.
<http://www.articuloz.com/empresas-articulos/la-importancia-de-la-auditoria-de-la-calidad-771130.html>
[Accedido de Noviembre 2014].

Blog - Asesor de Calidad >QUÉ SIGNIFICAN LAS SIGLAS: UNE, EN, ISO Y CTN.
<http://asesordecalidad.blogspot.com/2014/10/que-significan-las-siglas-une-en-iso-y.html#.VXIJAlLtmYw>
[Accedido el 27 de Abril de 2015].

Blog - Auditoría de Sistemas > CONTROL INTERNO INFORMATICO. SUS METODOS Y PROCESAMIENTOS. LAS HERRAMIENTAS DE CONTROL.
<https://noris14.wordpress.com/2011/06/10/control-interno-informatico/>
[Accedido el 3 de Noviembre de 2014].

Blog - ¿Cómo evaluar el l gobierno de las tecnologías y de los sistemas de información?
<http://consultoria-capacitacion-tic.blogspot.com.es/2014/05/como-evaluar-el-gobierno-de-las.html>
[Accedido el 21 de Junio de 2015].

Blog - Highlight > Guidance for organizations adopting the ISO/IEC 38500.
<https://blogs.ca.com/2009/02/23/guidance-for-organizations-adopting-the-iso-iec-38500/>
[Accedido el 8 de Octubre 2014].

Blog > Las Tecnologías de Información en la Organización.
<http://marcodegobdelasti.blogspot.com.es/>
[Accedido el 22 de Octubre de 2014].

Blog > Blog PUCP.
<blog.pucp.edu.pe>
[Accedido el 22 de Octubre de 2014].

Blog > IT – Governance, Risk & Compliance.
<https://francoitgrc.wordpress.com/2012/04/14/cobit-5-update-por-version-oficial-de-isaca/>
[Accedido el 27 de Septiembre de 2015].

Blogspot > Fundamentos de Gestión de Servicios T.I.
<http://fundamentosdegestiondeserviciosdeti.blogspot.com.es/>
[Accedido 12 de Diciembre de 2014].

Cintel > ARQUITECTURA EMPRESARIAL: UN NUEVO RETO PARA LAS EMPRESAS DE HOY.
<http://cintel.org.co/wp-content/uploads/2013/05/04.SOA_-_Eva_Maya.pdf>
[Accedido el 3 Mayo 2015].

CioIndex > Internal Auditor's Role in IT Governance.
<http://www.cioindex.com/it_governance/articleid/54805/internal-auditors-role-in-it-governance.aspx>
[Accedido el 13 de Octubre de 2014].

CMMI Institute.
<http://cmmiinstitute.com/about-cmmi-institute>
[Accedido el 16 de Marzo 2015].

Confecámaras > Qué es gobierno corporativo.
<http://www.confecamaras.org.co/gobierno-corporativo/165-que-es-gobierno-corporativo>
[Accedido el 6 de Diciembre de 2014].

Control Interno.
<http://veronicavafi.jimdo.com/app/download/7140526268/CONTROL%2BINTERNO.pdf?t=1358974842.>
[Accedido el 28 de Octubre de 2014].

Control interno y auditoría informática.
<es.slideshare.net/RobertoPorozo/control-interno-y-auditoria-informtica>
[Accedido el 18 de Noviembre de 2014].

COSO.
<http://www.coso.org/guidance.htm>
[Accedido el 19 de Abril de 2015].

COSO II – Internal Control Integrated Framework.
<http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf>
[Accedido el 19 de Abril de 2015].

Cuaderno ISACA.
<8-20710-05-06_ISACAMadrid - Cuaderno 0001_GBA_v01.00.pdf>
[Accedido el 22 de Abril 2015].

Definición del proceso de auditoría interna del aspecto adquisición, desarrollo y mantenimiento de sistemas de información para gestión de seguridad de la información soportado en TICs.
<repositorio.utp.edu.co/dspace/bitstream/11059/4119/1/0058M491D.pdf>
[Accedido el 26 de Octubre de 2014]

degerencia.com > Tecnología de Información.
<http://www.degerencia.com/tema/tecnologia_de_informacion>
[Accedido el 22 de Septiembre de 2014].

DELTA > Gobierno de TI: Respondiendo los cuatro "estamos".
<http://www.deltaasesores.com/articulos/negocios/5181-gobierno-de-ti-respondiendo-los-cuatro-estamos>
[Accedido el 3 de Octubre de 2014].

Docstoc > Auditoría de Tecnología de Información.
<http://www.docstoc.com/docs/28812966/AUDITORIA-DE-TECNOLOG%C3%8DA-DE-INFORMACI%C3%93N>
[Accedido el 22 de Septiembre de 2014].

Docstoc > Conceptos Básicos sobre Gobierno de Tecnologías de Información.
<http://www.docstoc.com/docs/3332971/Conceptos-Basicos-sobre-Gobierno-de-Tecnologias-de-Informacion>
[Accedido el 29 de Septiembre de 2014].

Docstoc > Metodología de la Auditoría Informática.
<http://www.docstoc.com/docs/21361749/METODOLOGIA-DE-LA-AUDITORIA-INFORMATICA>
[Accedido el 2 de Octubre de 2014].

Docstoc > Metodología de mejora continua y calidad total.
<http://www.docstoc.com/docs/21359294/METODOLOGIAS-DE-MEJORA-CONTINUA-Y-CALIDAD-TOTAL-AUDITORIA-DE>
[Accedido el 7 de Octubre de 2014].

educalibre.com > Norma UNE 71599-2:2010. Gestión de la continuidad del negocio. Parte 2: Especificaciones.
<http://www.educallibre.com/botiga/producte/10579/norma_une_71599-22010_gestion_de_la_continuidad_del_negocio_parte_2_especificaciones.html>
[Accedido el 3 de Abril 2015].

eHow en Español > Diferencia TIC.
<http://www.ehowenespanol.com/diferencia-tic-info_581848/>
[Accedido el 7 de Octubre de 2014].

El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento.
<http://www.ehu.eus/zer/hemeroteca/pdfs/zer27-14-cobo.pdf>
[Accedido el 3 de Octubre de 2014].

Gestiopolis.com > Tecnologías de información como claves del éxito.
<http://www.gestiopolis.com/canales3/ger/gertecventdes.htm>
[Accedido el 2 de Octubre de 2014].

Gestiopolis.com > Tecnologías de información y su utilidad en la empresa.
<http://www.gestiopolis.com/administracion-estrategia/estrategia/sistemas-y-tecnologias-de-la-informacion-2.htm>
[Accedido el 2 de Octubre de 2014].

Gobierno de las TI para las universidades.
<http://www.crue.org/Publicaciones/Documents/Gobierno%20TI/gobierno de_las_TI_para_universidades.pdf>
[Accedido el 2 de Octubre de 2014].

Grupo de Sistemas Inteligentes (GSI) > Las tecnologías de la información.
<http://www.gsi.dit.upm.es/~fsaez/intl/libro_complejidad/11-las-tecnologias-de-la-informacion.pdf>
[Accedido el 3 de Octubre de 2014].

Hammer >Process and Enterprise Maturity Model - (PEMM).
<http://www.hammerandco.com/HammerAndCompany.aspx?id=58>
[Accedido el 5 de Agosto 2015].

IAIA > ¿Qué quiere un buen auditor?
<http://www.iaia.org.ar/elauditorinterno/08/articulo3.html>
[Accedido el 16 de Diciembre 2014].

Implementing IT Governance.
<http://www.atilim.edu.tr/~mrehan/ISE511-Text.pdf>
[Accedido el 23 de Junio de 2015].

InformeTICfacil.com > ¿Qué son las TI?
<http://www.informeticplus.com/que-son-las-tecnologias-de-la-informacion>
[Accedido el 14 de Septiembre de 2014]

Instituto de Auditores Internos de Costa Rica > El Riesgo de Auditoría y sus Efectos sobre el Trabajo del Auditor Independiente.
<http://www.iaicr.com/audinotas/auditor_independiente.pdf>
[Accedido el 16 de Diciembre 2014].

Instituto de Auditores Internos de Costa Rica > ¿Dónde estaba el Auditor Interno?
<http://www.iaicr.com/audinotas/Donde_estaba.pdf>
[Accedido el 16 de Diciembre 2014].

INTOSAI > What is IT Governance and Why is it Important?
<http://www.intosaiitaudit.org/muscat/Canada-What_is_IT_Governance.pdf>
[Accedido el 23 de Junio de 2015].

ISACA.
<https://www.isaca.org/>
[Accedido el 19 de Abril de 2015].

ISACA> JOnline: Fundamentals of IT Governance Based on ISO/IEC 38500
<http://www.isaca.org/Journal/archives/2010/Volume-5/Pages/Fundamentals-of-IT-Governance-Based-on-ISOIEC-38500.aspx>
[Accedido el 07 de Agosto de 2015].

ISO 15504 para mejora y evaluación de procesos.
<http://www.softwcare.com/pdf/ISO%2015504%20para%20mejora%20y%20evaluaci%F3n%20de%20procesos.pdf>
[Accedido el 14 de Junio de 2015].

ISO/IEC 20000.Guía completa de aplicación para la gestión de los servicios de tecnologías de la información.
<PUB_DOC_Tabla_AEN_7172_1.pdf>
[Accedido el 12 de Diciembre de 2014].

ISO > Buscador de normas.
<http://www.iso.org/iso/search.htm?qt=ISO%2FIEC%2FIEEE+29119&sort_by=rel&type=simple&published=on&active_tab=standards>
[Accedido el 14 de Junio de 2015].

[ISO > ISO 12207:2008.
<http://www.iso.org/iso/catalogue_detail?csnumber=43447>
[Accedido el 6 Mayo 2015].

ISO > ISO/IEC 25000: 2005.
<http://www.iso.org/iso/catalogue_detail.htm?csnumber=35683>
[Accedido el 6 Mayo 2015].

ISO > ISO/IEC 25000:2014.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64764>
[Accedido el 14 de Junio de 2015].

ISO > ISO/IEC TR 29110-1:2011.
<http://www.iso.org/iso/catalogue_detail?csnumber=51150>
[Accedido el 6 Mayo 2015].

ISO 38500 IT Governance Standard.
<http://www.38500.org/>
[Accedido el 12 de Diciembre de 2014].

ISO/IEC JTC 1.
<http://www.iso.org/iso/jtc1_home.html>
[Accedido el 23 de Abril de 2015].

ISOTools > ISO 27001: Las TIC, más seguras que nunca.
<https://www.isotools.org/2014/11/25/iso-27001-tic-mas-seguras-que-nunca/#sthash.xDGNDQMe.dpbs>
[Accedido el 14 de Junio de 2015].

It Governance.
<http://www.itgovernance.co.uk/>.
[Accedido el 12 de Diciembre de 2014].

IT Governance and Process Maturity: A Field Study.
<http://www.computer.org/csdl/proceedings/hicss/2009/3450/00/09-10-10.pdf>
[Accedido el 23 de Junio de 2015].

IT Governance: Cobit 5.
<https://articulosit.files.wordpress.com/2013/07/it-governance-cobit-5.pdf>
[Accedido el 11 de Agosto de 2015].

IT Governance Drivers of Process Maturity.
<http://jebcl.com/symposium/wp-content/uploads/2011/08/Governance-Process-Maturity.pdf>
[Accedido el 23 de Junio de 2015].

ITIG.
<http://www.itgi.org/>
[Accedido el 23 de Abril de 2015].

ITIL Foundation - Gestión de servicios > Ciclo Deming.
<http://itilv3.osiatis.es/proceso_mejora_continua_servicios_TI/ciclo_deming.php>
[Accedido el 23 de Abril de 2015].

ITSM Portal > ISO38500.
<http://www.itsmportal.com/forum/iso-38500-not-low-hanging-fruit>
[Accedido el 19 de Abril de 2015].

Javier Garzas > ISO/IEC 29119.
<http://www.javiergarzas.com/2009/03/isoiec-29119-hacia-un-nueva-norma-para.html>
[Accedido el 22 de Mayo 2015].

La Contribución del Balanced Scorecard al Proceso de Gobierno de Tecnología de Información (TI).
<http://www.ucema.edu.ar/posgrado-download/tesinas2001/Rizzo-MADE.pdf>
[Accedido el 30 de Noviembre de 2014].

La Certificación por Niveles de Madurez de ISO/IEC 15504.
<http://www.kybeleconsulting.com/wp-content/uploads/2011/11/MCGarcia_CertificacionNivelesMadurez_ISO15504.pdf>
[Accedido el 19 de Junio de 2015].

Las herramientas de gestión del conocimiento. Una visión integrada.
<http://www.adingor.es/Documentacion/CIO/cio2004/comunicaciones/725-734.pdf>
[Accedido el 14 de Septiembre de 2014].

mailxmail.com > Curso elemental de auditoría - Capítulo 8: Atributos generales del auditor.
<http://www.mailxmail.com/curso-elemental-auditoria/atributos-generales-auditor>
[Accedido el 18 de Diciembre 2014].

monografias.com > Auditoría Informática.
<http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml>
[Accedido el 18 de Diciembre 2014].

monografias.com > DISEÑO DE UN MANUAL DE AUDITORÍA DE GESTIÓN.
<http://www.monografias.com/trabajos11/manaud/manaud.shtml>
[Accedido el 18 de Diciembre 2014].

monografias.com > Los sistemas de información y su importancia para las organizaciones y empresas.
<http://www.monografias.com/trabajos24/tics-empresas/tics-empresas.shtml>
[Accedido el 11 de Septiembre de 2014].

monografias.com > Sistema de Información.
<http://www.monografias.com/trabajos7/sisinf/sisinf.shtml>
[Accedido el 14 de Septiembre de 2014].

network sec > Auditoría IT Governance.
<http://www.network-sec.com/gobierno-TI/auditoria-IT-governance>
[Accedido el 28 de Diciembre 2014].

PdfSR.com > ISO/IEC 38500 vs. ISO/IEC 27000.
<http://pdfcast.org/pdf/iso-iec-38500-vs-iso-iec-27000>
[Accedido el 28 de Diciembre 2014].

PMBOK.
<http://temasselectossw.galeon.com/productos1835364.html>
[Accedido el 13 de Febrero de 2015].

Presentación - Tema 2 - Introducción a la auditoría de sistemas de información.
<http://www.dcc.etsii.urjc.es/sites/default/files/Presentacion - Tema 2 - Introduccion a la auditoria de sistemas de informacion.pdf>
[Accedido el 28 de Octubre de 2014].

Prezi >La norma/estándar UNE ISO/IEC 27001:2007.
<https://prezi.com/ru-p4odev1hh/la-normaestandar-une-isoiec-270012007-del-sistema-de-ges/>
[Accedido el 13 de Junio 2015].

PRINCE2.com > ¿Qué es PRINCE2?
<https://www.prince2.com/what-is-prince2>
[Accedido el 13 de Junio 2015].

Principios de Gobierno Corporativo de la OCDE, Organización para la Cooperación y el Desarrollo Económicos, 2004.
<http://www.oecd.org/daf/ca/corporategovernanceprinciples/37191543.pdf>
[Accedido el 30 de Noviembre de 2014].

Procesos Software ISO 15504:2004.
<http://procesosoftwareai.blogspot.com.es/2012/10/isoiec-155042004.html>
[Accedido el 22 de Mayo 2015].

Pruebas de Software ISO/IEC/IEEE 29119 Software Testing Standard.
<http://in2test.lsi.uniovi.es/gt26/?lang=es Grupo de Trabajo AEN/CTN71/SC7/GT26>
[Accedido el 22 de Mayo 2015].

Proyectos fin de carrera.com > La Auditoría.
<http://www.proyectosfindecarrera.com/que-es-una-auditoria.htm>
[Accedido en 2014].

QRP Internacional > ¿Qué es PRINCE2?
<http://www.qrpinternational.es/index/prince-2/what-is-prince2>
[Accedido el 1 Marzo de 2015].

Scientific Research - Implementing Good Governance Principles for the Public Sector in Information Technology Governance Frameworks.
<http://www.scirp.org/journal/PaperInformation.aspx?paperID=41979#.VRv5i8v3dZw.linkedin>
[Accedido el 13 de Agosto de 2015].

Slideshare >El Rol Del Auditor TI En La Gobernabilidad TI.
<http://www.slideshare.net/edays/el-rol-del-auditor-ti-en-la-gobernabilidad-ti>
[Accedido el 18 de Diciembre 2014].

Slideshare > Marcos de gobierno ti en las empresas.
<http://es.slideshare.net/rosmerybanr/marcos-de-gobierno-de-ti-41584821?next_slideshow=1>
[Accedido el 9 de Noviembre 2014].

Slideshare > Sistemas y Tecnologías de la Información.
<http://www.slideshare.net/profgloria/sistemas-y-tecnologias-de-la-informacin>
[Accedido el 14 de Septiembre de 2014].

Softwcare > ISO 15504 para mejora y evaluación de procesos.
<http://www.softwcare.com/pdf/ISO%2015504%20para%20mejora%20y%20evaluaci%F3n%20de%20procesos.pdf>
[Accedido el 18 de Agosto de 2015].

tcp > Gobierno IT.
<http://www.tcpsi.com/servicios/gobierno_ti.htm>
[Accedido 12 de Diciembre de 2014].

Tecnología Hecha Palabra > TI: Tecnologías de Información.
<http://www.tecnologiahechapalabra.com/tecnologia/glosario_tecnico/articulo.asp?i=875>
[Accedido el 9 de Noviembre 2014].

tics.
<http://uagro104vespertino.blogspot.com.es/2015/01/concepto-de-tegnologias-de-la.html>
[Accedido el 14 de Septiembre de 2014].

TOGAF Versión 9.1.
<http://www.vanharen.net/Samplefiles/9789087537104SMPL.pdf>
[Accedido el 11 Mayo 2015].

Tripod Blog > Auditoría de Sistemas.
<http://vbarreto.ve.tripod.com/keys/audi/audi01.html>
[Accedido el 14 de Septiembre de 2014].

Universidad Autónoma de México > importancia de la auditoría informática en las organizaciones.
<http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.htm>
[Accedido el 14 de Septiembre de 2014].

Universidad Complutense de Madrid > Influencia de las tecnologías de la información en los procesos de información y toma de decisiones de las empresas.
<http://www.ucm.es/info/multidoc/multidoc/revista/num10/paginas/pdfs/Apanos.pdf>
[Accedido 14 de Enero de 2015].

Universidad de Cuenca > Auditoría Informática.
<http://dspace.ucuenca.edu.ec/bitstream/123456789/652/3/ts205.pdf.txt>
[Accedido 14 de Enero de 2015].

Universitat Overta de Catalunya> Enfoque Comercial de la Fase de Definición de un Proyecto Informático.
<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/891/1/34954tfc.pdf>
[Accedido el 6 de Septiembre 2015].

Universidad Politécnica de Madrid > Cursos de verano UPM 2009.
<http://wn.com/Cursos_de_Verano_UPM_2009>
[Accedido 7 de Enero de 2015].

Universidad Politécnica de Valencia > Curso Gobierno TI Universidades.
<http://polimedia.upv.es/catalogo/curso.asp?curso=30b8dba7-d775-4b43-b5e8-2f49e7481bcd>
[Accedido el 18 de Agosto de 2015]

UOC > La tecnología de la información: herramienta esencial para gestionar la productividad.
<http://www.uoc.edu/symposia/euroecom/esp/art/homs0203/homs0203.html>
[Accedido 19 de Enero de 2015].

Val IT 2.0 – Valor Empresario: Gobierno de las Inversiones en TI.
<http://cafrancavilla.com/2009/08/08/val-it-2-0-valor-empresario-gobierno-de-las-inversiones-en-ti/>
[Accedido el 3 Mayo 2015].

Wiki.es > Procesos ITIL.
<http://wiki.es.it-processmaps.com/index.php/Procesos_ITIL>
[Accedido 27 de Enero de 2015].

Wikipedia > Centro de procesamiento de datos.
<http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos>
[Accedido el 17 Mayo 2015].

Wikipedia > Instituto Nacional Estadounidense de Estándares.
<http://es.wikipedia.org/wiki/Instituto_Nacional_Estadounidense_de_Est%C3%A1ndares
>
[Accedido el 19 de Abril de 2015]

Wikipedia > International Organization for Standardization.
<http://en.wikipedia.org/wiki/International_Organization_for_Standardization>
[Accedido en 2015].

Wikipedia > ISO/IEC 15504.
<http://es.wikipedia.org/wiki/ISO/IEC_15504>
[Accedido 07 de Junio de 2015].

Wikipedia > ISO/IEC 25000.
<http://es.wikipedia.org/wiki/ISO/IEC_25000>
[Accedido el 3 Mayo 2015].

Wikipedia > ISO/IEC JTC 1.
<http://en.wikipedia.org/wiki/ISO/IEC_JTC_1>
[Accedido el 3 Mayo 2015].

Wikipedia > Marco de Trabajo Zachman.
<http://es.wikipedia.org/wiki/Marco_de_Trabajo_Zachman>
[Accedido el 17 de Junio 2015].

Wikipedia > Norma UNE.
<http://es.wikipedia.org/wiki/Norma_UNE>
[Accedido el 27 de Abril de 2015].

Wikipedia > Project Management Institute.
<https://es.wikipedia.org/wiki/Project_Management_Institute>
[Accedido el 27 de Enero de 2015].

Wikipedia > TOGAF.
<https://es.wikipedia.org/wiki/TOGAF>
[Accedido el 11 Mayo 2015].

WordPress.com Blog > / IEC JTC 1 - La historia de JTC1.
<https://jtc1history.wordpress.com/>
[Accedido el 17 de Junio 2015].

WordPress.com Blog > Informando de Calidad - Definición de Auditoría de Calidad.
<http://informandodecalidad.wordpress.com/2008/04/09/definicion-de-auditoria-de-calidad/>
[Accedido el 4 de Febrero de 2015].

WordPress.com Blog > Gestión de Valor Inversiones en Tecnología - Waltzing with the Elephant – Por John Thorp.
<http://cafrancavilla.com/2009/11/04/waltzing-with-the-elephant-por-john-thorp/>
[Accedido el 17 de Noviembre de 2014].

WordPress.com Blog > PMQuality – IT Governance
<https://pmqlinkedin.wordpress.com/about/it-governace/>
[Accedido el 22 de Junio de 2015].

youtube.com > ISO 38500 Gobierno de TI o IT Governance. La Norma.
<http://www.youtube.com/watch?v=tA19jwv1SrU>
[Accedido el 29 de Septiembre de 2014].

Tesis Doctorales

Fernández, A.: "ANÁLISIS, PLANIFICACIÓN Y GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LAS UNIVERSIDADES". Universidad de Almería, 2009.

Lucio, T.:" Marco para la definición y adecuación de una service management office en el contexto de los servicios de tecnologías de la información". Universidad Carlos III de Madrid, 2013.

Pavez, A.: "Modelo de implantación de Gestión del Conocimiento y Tecnologías de Información para la Generación de Ventajas Competitivas". Valparaíso: Universidad Técnica Federico Santa María, 2000.

Rizzo, Mª E.: "La Contribución del Balanced Scorecard al Proceso de Gobierno de Tecnología de Información (TI)". Universidad del CEMA, 2001.

Santiago, D.: "Análisis y Estudio sobre el Gobierno y Gestión de los Servicios TI en el mercado español". Universidad Carlos III de Madrid, 2010.

Anexos

Anexo I **COBIT 5**
Anexo II **Val IT, cómo apoya al estándar UNE-ISO/IEC 38500**
Anexo III **Cuestionario Nivel de Capacidad**
Anexo IV **Cuestionario de Riesgos**
Anexo V **Prototipo del modelo de autoevaluación**

Anexo I - Resumen COBIT 5

A continuación, se presentan de forma resumida, los aspectos más relevantes de COBIT 5, extraído del documento "COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa", publicado por ISACA. (Para más detalle consultar el documento completo.)

Esta versión proporciona un marco para el gobierno y la gestión de las T.I en toda la empresa, incluyendo todas las áreas de negocio relacionadas con las T.I. Por tanto, su objetivo es ayudar a la creación de valor mediante las T.I, a través de su uso eficiente y la gestión optimizada de los riesgos y de los recursos.

COBIT 5 define para el gobierno de las T.I cinco principios clave y siete habilitadores, que se detallan a continuación:

Principio 1. Satisfacer las necesidades de las partes interesadas.

COBIT 5 permite a las organizaciones, mediante su conjunto de procesos definido, la generación de beneficios a través del uso de las T.I. El modelo de COBIT puede adaptarse a cualquier entidad en base a las metas definidas, relacionando estos objetivos con las metas T.I y estableciendo la correspondencia con los procesos de COBIT.

Principio 2. Cubrir la empresa extremo a extremo.

El marco considera todos los elementos de la empresa (recursos, funciones, procesos), que influyan en el gobierno y gestión de la T.I y donde la T.I es un activo más de la entidad.

Principio 3. Aplicar un marco de referencia único integrado.

COBIT 5 está alineado con otras normativas y marcos principales, de manera que puede utilizarse como marco orientativo para la gestión y gobierno de las T.I en una organización.

Principio 4. Hacer posible un enfoque holístico.

El marco incluye un conjunto de catalizadores que apoyan la implantación del gobierno y gestión T.I en una entidad, e impulsan la consecución de los objetivos empresariales. Se definen siete grupos de catalizadores:

- Principios, políticas y marcos de referencia: definen las pautas para alcanzar los objetivos propuestos.
- Procesos: son las actividades a través de las cuales se logran las metas T.I.
- Estructuras organizativas: son las encargadas de la toma de decisiones relevantes.
- Cultura, ética y comportamiento: son también factores decisivos que hay tener en cuenta para la garantizar el éxito del gobierno T.I.

- Información: es un activo clave necesario para mantener el funcionamiento y el buen gobierno de la organización.
- Servicios. Son los servicios, las aplicaciones y la infraestructura necesaria para el desarrollo e implementación de los procesos T.I
- Personas, habilidades y competencias: Las habilidades y las competencias de los recursos humanos son también activos necesarios para el desarrollo correcto de las distintas actividades que se llevan a cabo en una organización.

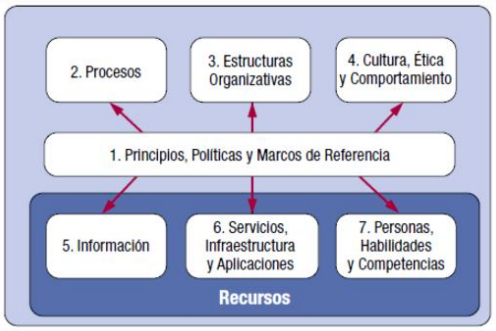

Figura 19. Catalizadores COBIT 5.

Principio 5. Separar el Gobierno de la Gestión.

Se separan los conceptos de gobierno y gestión. El gobierno se encarga de determinar los objetivos de la empresa y de definir y gestionar las actividades necesarias para conseguir estas metas empresariales. Por su parte la gestión se encarga de la planificación, ejecución y control de esas actividades.

En las siguientes figuras y a modo de resumen, se muestra el esquema de todos los procesos, tanto de gobierno como de gestión, que engloba COBIT 5 (Figura 20); y la comparativa de procesos entre la versión de COBIT 4 y COBIT 5, a la que se ha hecho mención en la memoria para justificar el descarte del modelo de madurez propuesto por COBIT 4 (Figura 21).

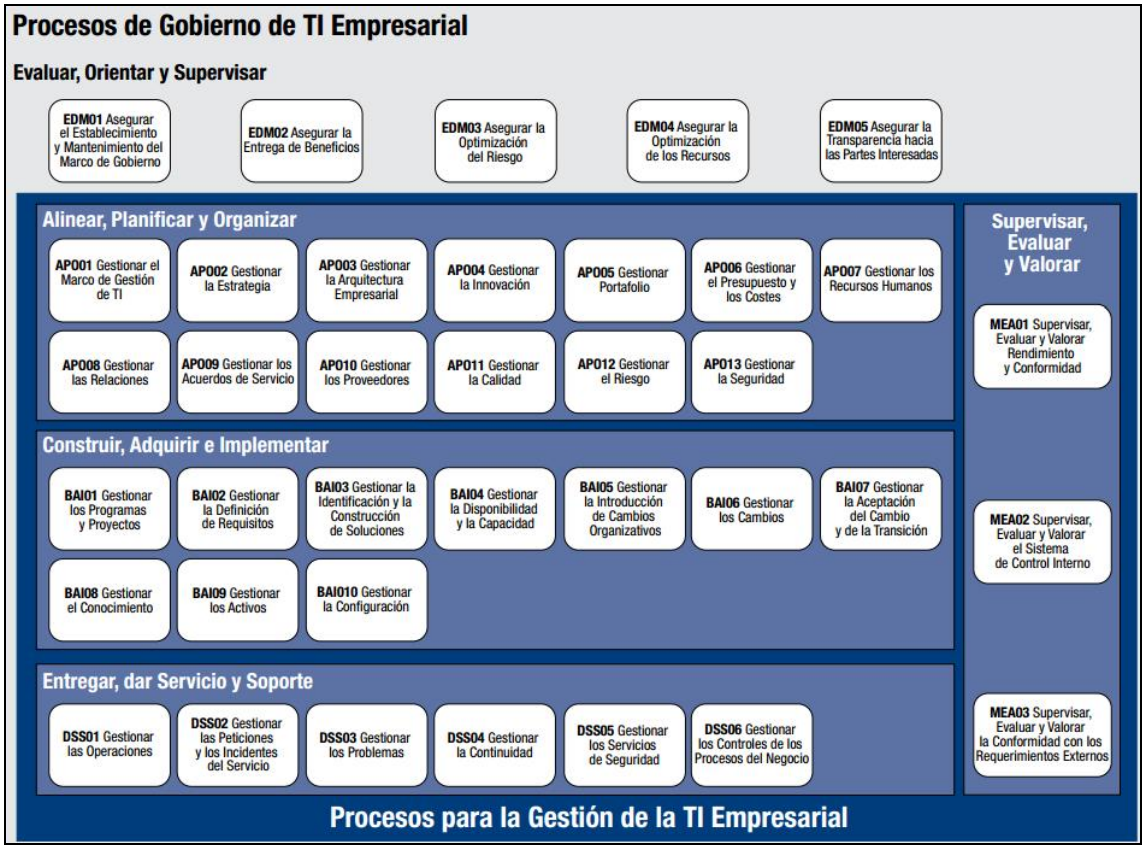

Figura 20. Procesos de COBIT.

COBIT 4.1		COBIT 5 - Cobertura (P)rimaria y (S)ecundaria	
Proceso	Descripción	Primaria	Secundaria
PO	Planear y Organizar	Alinear, Planear y Organizar	
PO1	Definir un plan estratégico de TI	APO02	EDM02 / APO05
PO2	Definir la arquitectura de la información	APO03	APO01
PO3	Definir la dirección tecnológica	APO02 / APO04	EDM01 / APO03 / APO01
PO4	Definir los procesos organización y relaciones de TI	APO01	APO07 / APO11 / DSS06
PO5	Administrar la inversión en TI	APO06	APO05
PO6	Comunicar las metas y la dirección de la gerencia	APO01	EDM03
PO7	Administrar los recursos humanos de TI	APO07	APO01
PO8	Administrar la calidad	APO11	
PO9	Evaluar y administrar los riesgos de TI	APO12	EDM03 / APO01
PO10	Administrar los proyectos	BAI01	
AI	Adquirir e Implementar	Construir, Adquirir e Implementar	
AI1	Identificar las soluciones automatizadas	BAI02	
AI2	Adquirir y mantener software aplicativo	BAI03	
AI3	Adquirir y mantener la infraestructura tecnológica	BAI03	DSS02
AI4	Facilitar la operación y el uso	BAI08	BAI05
AI5	Procurar recursos de TI	APO10	BAI03
AI6	Administrar los cambios	BAI06	
AI7	Instalar y acreditar las soluciones y cambios	BAI07	BAI05
DS	Entregar Servicio	Entregar Servicio y Soportar	
DS1	Definir y administrar los niveles de servicio	APO09	
DS2	Administrar los servicios de terceros	APO10	
DS3	Administrar el desempeño y la capacidad	BAI04	
DS4	Asegurar el servicio continuo	DSS04	
DS5	Garantizar la seguridad de los sistemas	DSS05	APO13
DS6	Identificar y asignar costos	APO06	
DS7	Educar y entrenar a los usuarios	APO07	
DS8	Administrar la mesa de servicio y los incidentes	DSS02	
DS9	Administrar la configuración	BAI10	DSS02
DS10	Administrar los problemas	DSS03	
DS11	Administrar los datos	DSS04	DSS01 / DSS05 / DSS06
DS12	Administrar el ambiente físico	DSS01 / DSS05	
DS13	Administrar las operaciones	DSS01	DSS05 / BAI09
ME	Monitorear y Evaluar	Monitorear y Evaluar	
ME1	Monitorear y evaluar el desempeño de TI	MEA01	
ME2	Monitorear y evaluar el control interno	MEA02	
ME3	Garantizar el cumplimiento regulatorio	MEA03	
ME4	Proporcionar gobierno de TI	EDM01 / EDM02 / EDM03 / EDM04 / MEA02	

Figura 21. Procesos de COBIT 4 vs COBIT 5. **[82]**

Para concluir, se detallan algunas de las **novedades** de COBIT 5:

- Usa un conjunto de praxis de gobierno y gestión que facilitan su implementación. También ha modificado su enfoque, pasando de una visión de objetivos a procesos.
- Está alineado con otros marcos y normas clave, por ejemplo, ITIL, ISO o PRINCE.
- Define una matriz de responsabilidades T.I más completa que la incluida en COBIT 4.1.
- No emplea el modelo de madurez de capacidad (CMMI), utilizado por ejemplo por Val IT o COBIT 4.1, sino que se basa en el modelo propuesto por la norma ISO/IEC 15504 para evaluar el nivel de capacidad de los procesos.

Anexo II - Val IT, cómo apoya al estándar UNE-ISO/IEC 38500

A continuación, se resume cómo Val IT y las guías relacionadas del ITIG apoyan la adopción de los principios y la implementación del estándar UNE-ISO/IEC 38500.

Principios del estándar:

Principio 1 - Responsabilidad.

La publicación "*Informe de la Junta de Gobierno de TI y Generación de Valor: Un Informe Ejecutivo sobre el Papel Crítico del Gobierno T.I*", proporciona orientación para el gobierno T.I sobre los roles y las responsabilidades, la función de T.I y describe cómo establecer un comité ejecutivo de T.I eficaz.

Otra publicación que apoya este principio es la "*Guía de Implementación de Gobierno TI: Usando COBIT y Val IT*", donde se detalla el papel de todas las partes interesadas y la forma de mejorar la estructura organizativa T.I.

Principio 2 – Estrategia.

La publicación "*Informe de la Junta de Gobierno de TI y Generación de Valor: Un Informe Ejecutivo sobre el Papel Crítico del Gobierno T.I*", explica cómo implementar una planificación estratégica T.I alineada con la planificación estratégica de toda la empresa, y cómo la Dirección del negocio y la de T.I deben cooperar para lograr los resultados.

El dominio IM – Investment Management, Gestión de la Inversión, proporciona guías para la gestión de inversiones T.I.

La publicación "*Identificando y Alineando las Metas de Negocio con las Metas T.I*", establece la relación entre los objetivos de negocio y los objetivos y procesos T.I.

Principio 3 – Adquisición.

Existen dos dominios de Val IT que apoyan este principio: El dominio IM, que orienta sobre aquellas inversiones T.I que pueden ser viables; y el dominio PM (Gestión de Portafolio), que indica cómo gestionar eficazmente las inversiones de la cartera de proyectos para obtener beneficios y optimizar los costes.

Principio 4 - Rendimiento (Desempeño).

Facilita una serie de ejemplos de métricas y objetivos aplicables a los procesos T.I e indica como relacionarlos con los objetivos de negocio. También incluye orientación para realizar el seguimiento del desempeño de la inversión de T.I.

Principio 5 - Conformidad.

La conformidad también implica decisiones de inversión. Val IT, específicamente a través de sus dominios VG (Gobierno del Valor) 1 y 3, PM (Gestión de Portafolio) 1 y 4, e IM (Gestión de la Inversión) 4, establece que las inversiones deben equilibrar la conformidad con el riesgo y con el coste de la no conformidad.

Principio 6 – Comportamiento humano.

El capítulo sexto de Val IT, *Responsabilidades y rendición de cuentas*, hace hincapié en la necesidad de entender el impacto en las inversiones T.I de los cambios de gobierno.

Sobre las **Tareas**:

Evaluar.

Las publicaciones "*Informe de la Junta de Gobierno de TI*" y "*Generación de Valor: Un Informe Ejecutivo sobre el Papel Crítico del Gobierno T.I*", describen el papel del consejo de dirección sobre el gobierno de la T.I: qué cubre, qué cuestiones deben preguntarse, y cómo comparar la propia empresa con las mejores prácticas.

Las fases *Identificación de necesidades* y *Visualizar la solución,* de la publicación "*Guía de Implementación de Gobierno TI: Usando COBIT y Val IT*", explican cómo focalizar la evaluación de la T.I en las necesidades del negocio y en los procesos críticos T.I.

La publicación "*Valor Empresarial: Gobierno de las Inversiones TI, Empezando con la Gestión del Valor*", ayuda a identificar factores generadores de valor y a evaluar las necesidades de negocio para mejorar la gestión de inversiones relacionadas con las T.I.

La publicación "*Valor Empresarial: Gobierno de las Inversiones TI, Los Casos de Negocio*", ayuda a conocer cuáles son las actividades necesarias para mejorar el gobierno de T.I.

Dirigir.

Las publicaciones "*Informe de la Junta de Gobierno de TI*" y "Generación *de Valor: Un Informe Ejecutivo sobre el Papel Crítico del Gobierno T.I*", describen las medidas que los consejos de dirección pueden aplicar sobre el gobierno de T.I,

Las fases *Planificar la solución* e *Implementar la solución* de la publicación "*Guía de Implementación de Gobierno TI: Usando COBIT y Val IT"*, explican cómo priorizar, planificar y diseñar las mejoras del gobierno T.I.

Monitorizar.

Las publicaciones "*Informe de la Junta de Gobierno de TI*" *y "Generación de Valor: Un Informe Ejecutivo sobre el Papel Crítico del Gobierno T.I*", describen las tareas de consejos de dirección para supervisar de manera eficaz el gobierno corporativo.

La fase *Implementar la solución* de la publicación "*Guía de Implementación de Gobierno TI: Usando COBIT y Val IT"*, explica cómo introducir el gobierno de T.I en las operaciones de negocio normales y cómo supervisar y medir el éxito de las mejoras en el gobierno de T.I.

Anexo III - Cuestionario Nivel de Capacidad

Niveles de capacidad							Procesos COBIT EDM				
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3 (Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)		EDM01	EDM02	EDM03	EDM04	EDM05
						Cuestionario					
						La empresa no necesita elaborar procesos de gobierno T.I.	x	x	x	x	x
						No existe ningún proceso relativo al gobierno T.I.	x	x	x	x	x
						No existen procesos para desarrollar o implantar el marco de gobierno T.I.	x				
						No se alcanza el valor óptimo de las iniciativas T.I, los servicios y los activos.	x				
						El modelo de toma de decisiones estratégico para T.I es eficaz y está alineado estrategia empresarial y con las exigencias de las partes interesadas (stakeholders).	x				
						El sistema de gobernanza para T.I está integrado en la empresa.	x				
						El sistema de gobernanza T.I funciona con eficacia.	x				
						No existen procesos que aseguren la entrega de beneficios.		x			

						La empresa asegura el valor óptimo de su cartera de proyectos o inversiones mediante iniciativas T.I, servicios y activos.		x			
						Se garantiza el valor óptimo de la inversión T.I a través de prácticas de gestión de valor efectivas.		x			
						La inversión T.I contribuye a incrementar el valor de negocio.		x			
						No existen procesos que aseguren la optimización del riesgo.			x		
						Están identificados los umbrales de riesgo y se conocen los principales riesgos asociados a las T.I.			x		
						La empresa gestiona los riegos críticos vinculados con las T.I de manera eficaz y eficiente.			x		
						No existen procesos que aseguren la optimización de recursos.				x	
						Los recursos que necesita la empresa están cubiertos de manera óptima.				x	
						Los recursos se asignan en base a las prioridades empresariales y siempre dentro de los límites presupuestados.				x	
						Se logra un uso óptimo de los recursos mediante ciclos de vida económicos completos.				x	
						No existen procesos que aseguren la transparencia de las partes interesadas.					x
						Los informes presentados por las partes interesadas están en línea con los requisitos definidos por los mismos.					x
						Los informes que se presentan son completos, se entregan a tiempo y son exactos.					x
						La comunicación es eficaz y las partes interesadas (stakeholders) están satisfechas.					x

Niveles de capacidad							Procesos COBIT 5 APO												
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3(Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)		APO01	APO02	APO03	APO04	APO05	APO06	APO07	APO08	APO09	APO10	APO11	APO12	APO13
						Cuestionario													
						No existen procesos para tratar el marco de gestión T.I.	x												
						Se definen y se mantienen políticas corporativas que cubren los requerimientos de gobierno corporativo.	x												
						Todo el mundo es consciente de las políticas corporativas y la forma en que se deben llevar a cabo.	x												
						No existen procesos que gestionen la estrategia empresarial.		x											
						La estrategia T.I está totalmente alineada con la estrategia empresarial.		x											
						La estrategia T.I es rentable, realista, alcanzable y está centrada en la empresa.		x											
						Se definen metas claras y alcanzables a corto plazo para lograr los requisitos definidos en la estrategia.		x											

						La Tecnología de la Información es un activo que aporta valor a la empresa.		x										
						Se conoce la importancia de definir una estrategia T.I.		x										
						La asignación de responsabilidades, para cumplir con las metas de la estrategia T.I, está bien definida.		x										
						No existen procesos que gestionen la arquitectura empresarial.			x									
						La arquitectura y los estándares utilizados apoyan de manera eficiente a la empresa.			x									
						Los servicios de arquitectura definidos permiten que los cambios puedan realizarse de forma ágil.			x									
						La arquitectura de la información es fiable y robusta.			x									
						No existen procesos para gestionar las actividades y procesos relacionados con la innovación.				x								
						Las soluciones tecnológicas empleadas por la empresa son las más adecuadas.				x								
						La identificación e implementación de los requisitos de empresa mediante el uso de soluciones innovadoras permite reducir costes y mejorar la calidad.				x								
						Existe una cultura empresarial de innovación.				x								

						No existen procesos para gestionar el portafolio.					x								
						La inversión a realizar está alineada con la estrategia empresarial.					x								
						Las fuentes de financiación de inversión están identificadas.					x								
						Se analizan y priorizan los casos de negocio antes de realizar cualquier inversión.					x								
						Existe una visión completa y precisa del desempeño de la cartera de inversiones.					x								
						Las modificaciones que se realicen en el plan de inversiones se reflejarán en las carteras de servicios T.I, en los activos y los recursos pertinentes.					x								
						Se supervisan los beneficios obtenidos.					x								
						No existen procesos encargados de la gestión del presupuesto y los costes.						x							
						Los presupuestos están disponibles, son detallados e incluyen todos los gastos previstos.						x							
						La asignación de los recursos T.I se priorizan en función a las necesidades de la entidad.						x							
						Los costes de los servicios se asignan de manera equitativa.						x							
						Los costes planificados están ajustados y coinciden con los costes reales.						x							

						No existen procesos para la gestión de los recursos humanos.							x						
						La inversión en recursos, formación, etc., realizada es acorde a las necesidades de la empresa.							x						
						La estructura organizacional es flexible.							x						
						Los recursos humanos se gestionan de manera eficaz y eficiente.							x						
						No existen procesos que gestionen los acuerdos de nivel de servicio.									x				
						Los servicios T.I funcionan correctamente y según lo establecido en el acuerdo de servicio (ANS).									x				
						Los acuerdos de nivel de servicio reflejan las necesidades empresariales y las capacidades de T.I.									x				
						No existen procesos para gestionar la relación con los proveedores.										x			
						Los proveedores actúan según lo acordado.										x			
						Antes de elegir un proveedor se evalúa el riesgo asociado y se toman las medidas correspondientes para que dicho riesgo no tenga un impacto negativo en la empresa.										x			
						Las relaciones con los proveedores son satisfactorias.										x			
						No existen procesos que aseguren la calidad.											x		

						Las partes interesadas (stakeholders) están satisfechas con el nivel de calidad de los servicios.											x		
						Los resultados de los proyectos y las entregas de los servicios son fiables.											x		
						En todos los procesos se implementan los criterios de calidad establecidos.											x		
						No existen procesos encargados de la gestión del riesgo.												x	
						Los riesgos relacionados con las T.I están identificados, analizados y son gestionados.												x	
						Existe un catálogo de riesgos.												x	
						Todas las tareas de gestión de riesgos están supervisadas.												x	
						Las acciones implementadas para gestionar los riesgos son eficientes.												x	

Niveles de capacidad							Procesos de COBIT 5 BAI									
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3 (Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)	**Cuestionario**	BAI01	BAI02	BAI03	BAI04	BAI05	BAI06	BAI07	BAI08	BAI09	BAI10
						No existen procesos que gestionen los programas y los proyectos.	x									
						Las partes interesadas (stakeholders) participan en los proyectos y programas.	x									
						Los resultados de los proyectos y de los programas logran los objetivos esperados.	x									
						Las tareas de los proyectos y de los programas se ejecutan según su planificación.	x									
						El número de recursos asignados a un programa o proyecto permite que no haya sobrecargas, retrasos, etc.	x									
						Se alcanzan los beneficios esperados de los programas y proyectos.	x									

						No existen procesos para gestionar la definición de requisitos.		x								
						Los requisitos funcionales y técnicos de negocio reflejan las necesidades y las expectativas de la empresa.		x								
						Las soluciones propuestas cubren la funcionalidad de negocio y los requisitos especificados.		x								
						Los riesgos derivados de los requisitos han sido abordados en las soluciones propuestas.		x								
						Los requisitos y las soluciones propuestas generan el valor esperado y están dentro del coste estimado.		x								
						No existen procesos encargados del establecimiento de soluciones.			x							
						El diseño de una solución satisface las necesidades de la empresa, cumple con la normativa y aborda todos los riegos identificados.			x							
						Cualquier solución llevada a cabo se ajusta al diseño y cumple con las normas de la organización. La solución implantada ha sido evaluada y supervisada.			x							
						Las soluciones son probadas y se garantiza su cumplimiento con los requisitos de calidad esperados.			x							
						Cualquier cambio en los requisitos definidos es incorporado correctamente en la solución propuesta.			x							
						No existen procesos para la gestión de cambios organizativos.					x					
						Los cambios propuestos o solicitados por las partes interesadas se tienen en consideración y se comprenden.					x					

						Existe un equipo encargado de gestionar los cambios.					x						
						El equipo encargado de gestionar los cambios es competente y logra abordarlos de manera eficiente.					x						
						Las tareas a realizar para implementar los cambios son entendidas y aprobadas por las partes interesadas.					x						
						Cualquier cambio se integra correctamente con el resto de los procesos o servicios.					x						
						No existen procesos encargados de gestionar la introducción de cambios.						x					
						Los cambios autorizados se realizan en plazo y con un número mínimo de errores.						x					
						Antes de llevar a cabo un cambio se realizan evaluaciones de impacto para identificar todos los componentes afectados.						x					
						Tras la realización de un cambio urgente se realiza siempre una supervisión del mismo.						x					
						Cuando se vaya a realizar un cambio se informa siempre a las partes principales afectadas.						x					
						No existen procesos para la implementación eficaz de los cambios.							x				
						Las pruebas de aceptación de los cambios son validadas por las partes interesadas. Además, estas pruebas tienen en cuenta todos los aspectos relativos a la implementación.							x				
						El pase a Producción de una mejora (release) se realiza con la intervención de las distintas partes interesadas.							x				

						Toda mejora (release) que se realice, se despliega correctamente, es estable y cumple con el objetivo de la misma.							x				
						Se documentan todos los aspectos de las releases: funcionalidad, pasos de implementación, despliegue, etc.							x				
						No existen procesos para gestionar y asignar el conocimiento a los recursos.								x			
						Están identificadas y clasificadas todas las fuentes de información.								x			
						La transferencia de conocimiento forma parte de la cultura empresarial.								x			
						Se realizan tareas/cursos de formación en base a los nuevos requerimientos.								x			

Niveles de capacidad							Procesos COBIT 5 DSS					
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3 (Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)		DSS01	DSS02	DSS03	DSS04	DSS05	DSS06
						Cuestionario						
						No existen tareas de control que garanticen la integridad de los procesos.						x
						Existen controles que permiten identificar los requisitos de negocio relativos al procesamiento de la información.						x
						La definición de roles, responsabilidades y accesos asignados se realizan en base a las autorizaciones de negocio.						x
						Todas las transacciones de negocio se registran en ficheros de traza (logs).						x
						El tiempo de permanencia de los ficheros de traza se define en base a la criticidad de los mismos, de manera que los que registren transacciones críticas serán permanentes.						x

Niveles de capacidad							Procesos COBIT 5 MEA		
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3 (Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)		MEA01	MEA02	MEA03
						Cuestionario			
						No hay definidas actividades encargadas de la evaluación del rendimiento y de la conformidad de los procesos respecto a los objetivos definidos.	x		
						Existe conformidad de las partes interesadas sobre las metas y las métricas a emplear.	x		
						La medición de los procesos se realiza respecto a las métricas y a los objetivos acordados.	x		
						Las tareas de supervisión y evaluación son eficaces.	x		
						Los objetivos y las métricas de negocio están integrados en los procesos de monitorización.	x		
						Se realizan informes de rendimiento y conformidad.	x		
						Se comprende la utilidad de los informes de rendimiento y conformidad.	x		
						No existen procesos encargados de la supervisión, evaluación y valoración de los controles internos.		x	

						Los procesos, los recursos y la información están incluidos como requisitos del sistema de control interno de la empresa.		x	
						Las iniciativas y medidas de control son planificadas y ejecutadas con eficacia.		x	
						El sistema de control interno ha sido evaluado por una entidad independiente que garantiza su eficacia.		x	
						Las deficiencias identificadas por los controles internos se registran y se reportan.		x	
						No existen procesos encargados de la supervisión, evaluación y valoración de los requisitos externos.			x
						Se identifican todos los requisitos externos que hay que cumplir.			x
						Los requisitos de cumplimiento externos se tratan y gestionan adecuadamente.			x

Niveles de capacidad							Procesos COBIT 5				
Nivel 0 (Proceso Incompleto)	Nivel 1 (Proceso Ejecutado)	Nivel 2 (Proceso Gestionado)	Nivel 3 (Proceso Establecido)	Nivel 4 (Proceso Predecible)	Nivel 5 (Proceso Optimizado)	**Cuestionario**	Dominio EDM	Dominio AP0	Dominio BAI	Dominio DSS	Dominio MEA
						Están identificados los requisitos de desarrollo del proceso.	x	x	x	x	x
						Las tareas de desarrollo del proceso están planificadas y son supervisadas.	x	x	x	x	x
						El comportamiento del proceso se ajusta a la funcionalidad establecida.	x	x	x	x	x
						Los roles y responsabilidades relativas al proceso han sido establecidas y comunicadas.	x	x	x	x	x
						El proceso cuenta con la información y los recursos necesarios para su desarrollo.	x	x	x	x	x
						Existe un canal de comunicación eficaz entre las partes implicadas de cada proceso.	x	x	x	x	x
						Están identificadas las salidas del proceso.	x	x	x	x	x
						Están identificados los requisitos de documentación y de control de las salidas del proceso.	x	x	x	x	x
						Las salidas de los procesos están correctamente identificadas, documentadas y controladas.	x	x	x	x	x

						Las salidas del proceso se ajustan a los requerimientos definidos.	x	x	x	x	x
						Existe un proceso estándar que define los elementos fundamentales que deben ser incorporados en el proceso definido.	x	x	x	x	x
						En el estándar está definida la relación e interactuación del proceso con otros procesos.	x	x	x	x	x
						Los roles y las responsabilidades están también incluidas en el proceso estándar.	x	x	x	x	x
						La infraestructura requerida está definida en el proceso estándar.	x	x	x	x	x
						Está monitorizado el proceso para comprobar su nivel de efectividad y adecuación.	x	x	x	x	x
						El proceso se despliega en base al proceso estándar.	x	x	x	x	x
						Se asignan al proceso, los roles, responsabilidades y autoridades requeridas.	x	x	x	x	x
						Los recursos que desarrollan el proceso son competentes y tienen la formación necesaria para llevar a cabo esta tarea.	x	x	x	x	x
						La infraestructura necesaria para el desarrollo del proceso está disponible y se realizan tareas para su mantenimiento y actualización.	x	x	x	x	x
						El proceso está documentado e incluye la forma en la que el proceso apoya los objetivos de negocio.	x	x	x	x	x
						Los objetivos o indicadores para medir el proceso se obtienen a partir de las necesidades de información del proceso.	x	x	x	x	x
						Se definen los objetivos cuantitativos para el funcionamiento de proceso utilizando como base los objetivos relevantes de negocio.	x	x	x	x	x
						Están identificados los criterios y la frecuencia de medición, así como los objetivos a medir para el funcionamiento del proceso.	x	x	x	x	x

						Los resultados de las mediciones son recogidos, analizados y reportados con el fin de monitorizar los objetivos para asegurar el funcionamiento de proceso.	x	x	x	x	x
						Los resultados de las mediciones son usados para determinar el funcionamiento de proceso.	x	x	x	x	x
						Se han definido técnicas de control y análisis para el proceso y estas son las que se utilizan.	x	x	x	x	x
						Están establecidos los límites de variación de los resultados de las mediciones, dentro de los cuales se asegura el funcionamiento normal del proceso.	x	x	x	x	x
						Los datos de las mediciones realizadas en el proceso se analizan para determinar el origen de las variaciones anormales.	x	x	x	x	x
						Si el resultado de la medición del proceso está fuera de los márgenes de variación establecidos, se llevan a cabo acciones correctivas.	x	x	x	x	x
						Cuando se aplica una acción correctiva sobre un proceso se garantiza que el proceso sigue funcionado correctamente y que, ahora, sus resultados están dentro de los márgenes de valores correctos.	x	x	x	x	x
						Los objetivos de mejora del proceso se establecen en base a los objetivos más relevantes del negocio.	x	x	x	x	x
						Están recopiladas las causas comunes que originan variaciones en el funcionamiento de proceso. Existe un proceso continuo de análisis de datos para identificar estas causas.	x	x	x	x	x
						Existe una tarea continua de análisis de datos para mejorar y poder introducir innovaciones en el proceso.	x	x	x	x	x
						Se analizan e identifican aquellas tecnologías y desarrollos que pueden optimizar el proceso.	x	x	x	x	x
						Existe un proceso de mejora continua.	x	x	x	x	x
						Los cambios propuestos son evaluados para ver si generan impacto sobre la funcionalidad y finalidad del proceso.	x	x	x	x	x
						Está identificada cualquier interrupción, que afecte al funcionamiento normal del proceso, originada	x	x	x	x	x

						por la implementación de cualquier cambio. Existe un mecanismo de contingencia para recuperar la normalidad del proceso.					
						Tras la implementación de un cambio en el proceso se evalúa la eficacia del mismo, para determinar si los resultados obtenidos son debidos al cambio o a alguna causa especial.	x	x	x	x	x

Anexo IV - Cuestionario de Riesgos

Papel del Consejo en relación a las Tecnologías de Información.

Cuestión	Riesgos	Controles
¿Está especificada y definida la finalidad de la empresa?	• Estrategia no definida. • Los objetivos definidos no son claros ni son los adecuados para la consecución de las metas de la organización. • Desubicación sectorial.	• Establecimiento de la misión de la organización. • Definición de los objetivos estratégicos.
¿Hay una estructura organizativa definida?	• No se pueden definir roles ni responsabilidades. • Duplicidad de las competencias definidas. • Esfuerzos duplicados.	• Diseñar e implementar una estructura organizativa y definir las funciones y responsabilidades de cada miembro.
¿Se ha definido una matriz de responsabilidades?	• No se conocen cuáles son las obligaciones a cumplir ni quién debe llevarlas a cabo. • No se cumple con la normativa.	• Informar sobre las consecuencias del incumplimiento de sus obligaciones y realizar las tareas formativas correspondientes.
¿Es el Consejo el encargado de las tareas de gobierno T.I?	• Dirección inexistente.	• Diseñar e implementar una estructura organizativa y definir las funciones y responsabilidades de cada miembro.
¿La Dirección establece los objetivos de negocio?	• Metas de negocio inalcanzables.	• Determinar las metas empresariales.
¿Los usuarios conocen sus responsabilidades?	• No queda claro cuál es el objetivo a realizar en la tarea asignada • Acceso y uso no autorizado de la información. • La imagen de la empresa puede resultar dañada.	• Diseñar e implementar una estructura organizativa y definir las funciones y responsabilidades de cada miembro. • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas.

¿Se dispone de los recursos necesarios?	• Metas de negocio inalcanzables. • Incremento del estrés laboral. • Se produce la desmotivación de los trabajadores.	• Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias.
¿Se realiza un uso eficiente de los recursos?	• Gestión de recursos ineficiente.	• Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias.
¿Participan los departamentos involucrados en todas las etapas de desarrollo de los procesos?	• Metas de negocio inalcanzables. • Los sistemas no permiten satisfacer los requisitos empresariales	• Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas. • Comunicar a todos los departamentos la importancia de definir correctamente sus requerimientos y de su participación para la consecución de los objetivos de negocio.
¿Se informa a la Dirección sobre las ventajas, a nivel competitivo, de la inversión en nuevas tecnologías?	• No se aprovecha la capacidad estratégica de las T.I. • Pérdida de capacidad competitiva. • No se puede hacer frente a todos los cambios del entorno.	• Se debe asignar a las T.I el mismo valor en el Consejo que al resto de departamentos y activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo.
¿Está la Dirección informada sobre los riegos vinculados al uso de la T.I?	• Toma de decisiones incorrectas.	• Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo.

¿Existe en la empresa un marco para a la gestión de riesgos?	• Incapacidad para identificar todos los riesgos que ponen en peligro el alcance de las metas.	• Los riesgos deben ser gestionados por su área correspondiente afectada. • La Dirección debe evaluar de forma periódica los riesgos.
¿Están establecidos los niveles de riesgo que la empresa puede asumir sin que estos afecten a su rendimiento y cumplimiento?	• Incapacidad para alcanzar los objetivos definidos.	• Se deben definir las situaciones en las que los riesgos son asumibles. • Es tarea de cada área identificar y llevar a cabo las medidas correctivas necesarias para sus riesgos.

Papel de la Tecnología de la Información en la organización.

Cuestión	Riesgos	Controles
¿La función de la T.I es clara?	• La estrategia de negocio no está alineada con la de T.I. • No se aprovecha la capacidad estratégica de las T.I. • Incapacidad para evaluar el desempeño.	• Deben utilizarse herramientas para la asignación de responsabilidades y para la medición del rendimiento. • Hay que definir indicadores para medir el desempeño.
¿Existe una estructura organizativa que gestione la T.I?	• Problemas para diseñar de los objetivos y estrategias T.I. • La estructura organizativa no puede soportar los objetivos de negocio. • No se puede hacer frente a todos los cambios del entorno.	• Revisar la estructura organizativa T.I y realizar los cambios necesarios para poder cumplir con los requisitos de negocio y poder hacer frente a los cambios.
¿Se ha definido una matriz de responsabilidades T.I?	• Uso ineficiente de recursos. • Capacidad de innovación limitada. • Procesos inestables y con poco rendimiento.	• Se debe elegir una metodología acorde con el tipo de proyectos que se llevan a cabo. • Todos los departamentos de la entidad deben seguir la metodología elegida para optimizar su nivel de madurez.
¿Hay alguna metodología o marco de trabajo definida?	• Imposibilidad de implantar estándares de trabajo.	• Se debe elegir una metodología acorde con el tipo de proyectos que se llevan a cabo. • Todos los departamentos de la entidad deben seguir la metodología elegida para optimizar su nivel de madurez.
¿Se redactan informes de seguimiento?	• Imposibilidad de definir y aplicar medidas correctivas.	• Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario.
¿La Dirección conoce las desviaciones detectas en los informes de seguimiento?	• Gestión poco eficiente de los recursos.	• Se debe elegir una metodología acorde con el tipo de proyectos que se llevan a cabo. • Todos los departamentos de la entidad deben seguir la metodología elegida para optimizar su nivel de madurez.

¿Están identificadas las causas que producen las desviaciones?	• No se identifican ni corrigen las desviaciones. • La entidad no puede crecer. • Incapacidad para llevar a cabo proyectos nuevos o de carácter innovador.	• Se debe elegir una metodología acorde con el tipo de proyectos que se llevan a cabo. • Todos los departamentos de la entidad deben seguir la metodología elegida para optimizar su nivel de madurez.
¿Hay definido un plan de actuación para corregir las desviaciones?	• Pérdida de capacidad competitiva. • Pérdida de oportunidades.	• Definir los objetivos de negocio, identificar y corregir las desviaciones para que los resultados obtenidos cumplan las especificaciones definidas en los objetivos.
¿Las decisiones tomadas a corto plazo afectan a la estrategia de negocio?	• La imagen de la empresa puede resultar dañada. • No se cumple con la normativa. • Sanciones de carácter administrativo para la empresa. • Acceso y uso no autorizado de la información.	• Elaborar y actualizar el régimen de uso de los recursos T.I.
¿Los usuarios conocen la normativa relacionada con el uso de la T.I?	• La imagen de la empresa puede resultar dañada. • No se cumple con la normativa. • Sanciones de carácter administrativo para la empresa • Acceso y uso no autorizado de la información.	• Determinar el impacto del no cumplimiento de las obligaciones. • Diseñar e implementar una estructura organizativa y definir las funciones y responsabilidades de cada miembro. • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas.
¿Los usuarios están al tanto de los riesgos y efectos derivados del incumplimiento normativo?	• La imagen de la empresa puede resultar dañada. • No se cumple con la normativa. • Sanciones de carácter administrativo para la empresa. • Acceso y uso no autorizado de la información.	• Elaborar y actualizar el régimen de uso de los recursos T.I.
¿La introducción de nuevos recursos T.I lleva consigo la actualización de la normativa relacionada con su uso?	• La imagen de la empresa puede resultar dañada. • No se cumple con la normativa. • Sanciones de carácter administrativo para la empresa. • Acceso y uso no autorizado de la información.	• Elaborar y actualizar el régimen de uso de los recursos T.I.

Los cambios incorporados se comunican a los usuarios para que estén al tanto de los mismos.	• La gestión incorrecta de recursos provoca que los cambios no lleguen a implementarse. • Los cambios no se implantan de forma correcta.	• Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias.
¿Se cuenta con los recursos indispensables para llevar a cabo cualquier tecnológico?	• No aprovechamiento de las oportunidades asociadas al cambio por falta de recursos. • Se rechazan los cambios aunque su implementación pueda generar valor.	• Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas. • Comunicar a todos los departamentos la importancia de definir correctamente sus requerimientos y de su participación para la consecución de los objetivos de negocio.
¿Se explica a los usuarios la necesidad del cambio?	• Los cambios son considerados obstáculos y no se aprecia la generación de valor que conllevan. • Se rechazan los cambios aunque su implementación pueda generar valor.	• Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas. • Comunicar a todos los departamentos la importancia de definir correctamente sus requerimientos y de su participación para la consecución de los objetivos de negocio.
¿Se explican a los usuarios los beneficios del cambio?	• Los cambios son considerados obstáculos y no se aprecia la generación de valor que conllevan. • Se rechazan los cambios aunque su implementación pueda generar valor.	• Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas. • Comunicar a todos los departamentos la importancia de definir correctamente sus requerimientos y de su participación para la consecución de los objetivos de negocio. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo.

¿Cuándo se realiza un proceso de cambio existe una vía de comunicación interdepartamental?	• Gestión de recursos ineficientes. • Las intervenciones de los departamentos no están coordinadas.	• Definir canales de comunicación efectivos.
¿Los usuarios están conformes con el desempeño de T.I?	• Los proyectos futuros no cuentan con el respaldo de los usuarios. • La T.I no es percibida como un facilitador.	• Solicitar mediante encuestas su opinión a los usuarios. • En base a las encuestas revisar y mejorar la gestión de la T.I.

Principio de ESTRATEGIA

Cuestión	Riesgos	Controles
¿El responsable T.I es miembro de la Dirección?	• Los objetivos de negocio y los de T.I no están alineados. • No se cuenta con el respaldo de la Dirección.	• Incluir en el comité a los responsables T.I.
¿Los responsables T.I pueden intervenir en las decisiones estratégicas?	• Los objetivos de negocio y los de T.I no están alineados.	• Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Se debe elegir una metodología acorde con el tipo de proyectos que se llevan a cabo.
¿Se informa al responsable T.I sobre los planes empresariales?	• Los objetivos de negocio y los de T.I no están alineados.	• Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo.
¿Los planes de negocio y los de T.I están alineados?	• Los objetivos de negocio y los de T.I no están alineados.	• Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Supervisar los planes.
¿Se mide el desempeño de las T.I y su relación con la consecución de objetivos de la entidad?	• No existe forma de saber si se han alcanzado o si se cumplen las metas de la organización. • Gestión poco eficiente de los recursos T.I.	• Definir un conjunto de indicadores para evaluar el repercusión y el rendimiento de los requisitos empresariales.
¿Las decisiones T.I se realizan en base a los resultados de los indicadores de seguimiento?	• Los objetivos de negocio y los de T.I no están alineados. • No se cuenta con el respaldo de la Dirección.	• Determinar las metas empresariales.

¿La Dirección está al tanto del resultado de los informes de seguimiento?	• Los objetivos de negocio y los de T.I no están alineados. • No se cuenta con el respaldo de la Dirección.	• Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo.
¿Se ha definido una metodología para las tareas de planificación, gestión de riesgos y definición y consecución de los objetivos empresariales?	• Los objetivos de negocio y los de T.I no están alineados. • No se cuenta con el respaldo de la Dirección. • No existe forma de saber si se han alcanzado o si se cumplen las metas de la organización. • Gestión poco eficiente de los recursos T.I. • Costes elevados, incluso no asumibles.	• Se debe elegir una metodología acorde con el tipo de proyectos que se llevan a cabo. • Todos los departamentos de la entidad deben seguir la metodología elegida para optimizar su nivel de madurez.
¿La Dirección aprueba los planes T.I?	• Los objetivos de negocio y los de T.I no están alineados. • No se cuenta con el respaldo de la Dirección.	• Definición de los objetivos estratégicos. • Determinar las metas empresariales. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo.

Principio de ADQUISICIÓN (INVERSIÓN)

Cuestión	Riesgos	Controles
¿La inversión T.I se realiza en base al análisis estratégico de la Dirección?	• La T.I no se han dimensionado correctamente. • Los objetivos de negocio y los de T.I no están alineados	• Definición de los objetivos estratégicos. • Determinar las metas empresariales. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo.
¿Se dispone de un Plan de Infraestructura Tecnológica?	• Las exigencias de los usuarios se ejecutan con demora. • La falta de innovación T.I puede provocar la pérdida de oportunidades.	• Determinar las metas empresariales.
¿Se realizan revisiones del plan de infraestructura tecnológica?	• Las exigencias de los usuarios se ejecutan con demora. • La falta de innovación T.I puede provocar la pérdida de oportunidades.	• Determinar las metas empresariales. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo. • Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario.

¿A la hora de elaborar la infraestructura tecnológica se tienen en cuenta las tendencias y la normativa aplicable?	• Capacidad de innovación limitada. • No se cumple con la normativa.	• Determinar las metas empresariales. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo. • Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario. • Conocer y seguir la normativa aplicable.
¿Antes de adquirir una nueva tecnología se analiza su impacto?	• Los sistemas actuales de la organización pueden ver afectado su funcionamiento tras la incorporación de una tecnología.	• Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario. • No realizar inversiones tecnológicas sin leer previamente los informes correspondientes.
¿Se tienen en cuenta aspectos como la adecuación, evolución, etc., de la infraestructura, en el plan tecnológico?	• Interrupción de los servicios. • Riesgo de quiebra de la entidad.	• Elaborar y mantener un plan para el mantenimiento la infraestructura tecnológica.
¿Se realizan y planifican tareas de mantenimiento tecnológico?	• Existen procesos claves que están sostenidos por tecnologías desfasadas.	• Elaborar y mantener un plan para el mantenimiento la infraestructura tecnológica. • Evaluar de forma periódica la infraestructura para conocer su estado.

¿Existen un entorno de pruebas?	• La omisión de pruebas puede provocar que, al implantar una aplicación en producción, se produzcan fallos o interrupciones en el servicio. • Al no realizar pruebas, no se garantiza el resultado de las aplicaciones.	• Definir un plan de pruebas, que garantice los resultados y la operatividad del sistema. • Las implantaciones en producción deben incluir una fase de pruebas en dicho entorno.
¿La Dirección interviene en las tareas de adquisición?	• Se realizar inversiones no alineadas con las necesidades del negocio.	• Elaborar un plan de adquisición.

Principio de RENDIMIENTO

Cuestión	Riesgos	Controles
¿La estimación de los recursos T.I es correcta y permite alcanzar los objetivos de negocio?	• Metas de negocio inalcanzables. • Incremento del estrés laboral. • Riesgo de quiebra de la entidad.	• Determinar las metas empresariales. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo. • Los informes redactados tienen que ser concretos, contener la información justa y estar redactados de forma sencilla, de manera que sean comprensibles para cualquier usuario. • Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias.
¿Se llevan a cabo auditorías para evaluar el rendimiento de los procesos T.I?	• Los recursos son gestionados de forma poco eficiente.	• Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Evaluar mediante auditorías el rendimiento de los procesos T.I.
¿Se evalúa si el nivel de servicio actual es el acordado?	• No existe forma de saber si se han alcanzado o si se cumplen las metas de la organización.	• Definir un conjunto de indicadores para evaluar la repercusión y el rendimiento.
Cuando se llevan a cabo mejoras, ¿se mide su grado de conformidad o rendimiento?	• Las desconformidades no solventan.	• Realizar auditorías para evaluar el rendimiento.

Se realizan evaluaciones externas para medir el nivel de rendimiento de las T.I.	• Toma de decisiones no objetivas. • No se detectan las ineficiencias.	• Realizar auditorías externas.
¿Los informes de rendimiento T.I, que recibe la Dirección, incluye el grado de cumplimiento de las mismas?	• Metas de negocio inalcanzables. • No se cumplen con los requerimientos de todas las partes interesadas.	• Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Las T.I deben tener para la Dirección el mismo peso que el resto de activos. • Para la toma correcta de decisiones T.I deben conocerse la estrategia y los objetivos actuales y a largo plazo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo.
¿Se planifica la capacidad T.I?	• No se tienen los recursos humanos suficientes y necesarios. • Los recursos humanos no tienen los conocimientos necesarios.	• Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias.
¿Se revisa si el uso de las T.I que realizan los usuarios es correcto?	• No se cumple con la normativa. • No se cumplen los objetivos de negocio. • Gestión no adecuada de los recursos.	• Intentar automatizar los procesos. • Formar a los recursos.
¿Están contemplados en los niveles de servicio el nivel mínimo de rendimiento T.I?	• Los objetivos de negocio y los de T.I no están alineados.	• La definición del ANS debe realizarla los responsables T.I. • Resolver los conflictos de intereses.
¿Se mide el rendimiento de los servicios externos?	• Los objetivos de negocio y los de T.I no están alineados. • Incumplimiento del nivel de servicio.	• La entidad externa debe presentar informes de rendimiento. • Realizar encuestas de satisfacción a las empresas contratantes.

¿Hay algún tipo de medida de control que asegure la integridad de la información T.I?	• No se cumple con la normativa. • Otras organizaciones puede resultar afectadas.	• Garantizar que las medidas de control son efectivas. • Determinar un nivel de prioridad a los procesos y servicios, para saber cuáles son los más críticos y sobre cuales reforzar los controles. • Determinar las metas empresariales. • Crear conciencia sobre la necesidad de la seguridad de la información.
¿Existe un plan ante contingencias, y este plan garantiza el nivel de servicio?	• Interrupción de los servicios. • Riesgo de quiebra de la entidad.	• Elaborar y mantener un plan para mantener la infraestructura tecnológica. • Realizar de manera periódica pruebas, para detectar anomalías y evaluar la eficacia del plan de contingencias. • En base a los resultados de las pruebas realizar los cambios correspondientes.
¿Se poseen los conocimientos y medios suficientes para solventar las contingencias T.I de forma eficiente?	• Interrupción de los servicios. • Riesgo de quiebra de la entidad.	• Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Llevar a cabo tareas de formación a los recursos.
¿Se lleva a cabo algún tipo de tarea para corregir las desviaciones de rendimiento detectadas en los niveles de servicio?	• Interrupción de los servicios. • Riesgo de quiebra de la entidad.	• Evaluar si el nivel de servicio es el acordado. • Adaptar los acuerdos de nivel de servicio a las necesidades de las partes interesadas y los cambios T.I introducidos. • La definición del ANS debe realizarla los responsables T.I. • Resolver los conflictos de intereses.

Principio de CONFORMIDAD

Cuestión	Riesgos	Controles
¿Se comprende cuáles son las normas generales y las del sector que hay cumplir?	• Sanciones económicas que pueden afectar al patrimonio de la entidad. • Se daña la imagen corporativa. • La entidad debe cesar su actividad.	• Estudiar la normativa aplicable. • Determinar cada normativa a que procesos aplica. • Dar formación en materia normativa a los encargados de los procesos. • Realizar auditorías para evaluar el grado de cumplimiento.
¿Está garantizado el uso de la información solo con carácter laboral?	• Sanciones económicas que pueden afectar al patrimonio de la entidad. • Se daña la imagen corporativa. • La entidad debe cesar su actividad.	• Definir cláusulas de uso de la información en los contratos. • Garantizar la confidencialidad de la información y aplicar las medidas o controles para asegurarlo.
¿Se informa al personal sobre el tratamiento y la confidencialidad de la información y de los recursos?	• Sanciones económicas que pueden afectar al patrimonio de la entidad. • Se daña la imagen corporativa. • La entidad debe cesar su actividad.	• Informar sobre las consecuencias del Incumplimiento de las obligaciones. • Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Diseñar e implementar una estructura organizativa y definir las funciones y responsabilidades de cada miembro • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas.
¿Se realiza algún tipo de auditoría para determinar si a nivel interno se cumple la normativa?	• Sanciones económicas. • Se daña la imagen corporativa. • Se pueden perder clientes.	• Realizar auditorías de manera periódica.

¿Se comprueba si las anomalías detectadas en las auditorías son corregidas?	• Las desconformidades no se solventan.	• Llevar a cabo tareas de verificación para saber si las recomendaciones de las auditorías se han aplicado.
¿Los empleados conocen que el Incumplimiento del uso de la T.I puede conllevar un delito legal, que afectará a la empresa?	• Sanciones económicas que pueden afectar al patrimonio de la entidad. • Se daña la imagen corporativa. • La entidad debe cesar su actividad.	• Diseñar e implementar una estructura organizativa y definir las funciones y responsabilidades de cada miembro. • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas.
¿Se revisan los sistemas, procesos, etc., para garantizar que cumplen la normativa?	• Sanciones económicas que pueden afectar al patrimonio de la entidad. • Se daña la imagen corporativa. • La entidad debe cesar su actividad.	• Revisar los sistemas, los procesos, etc. • Realizar auditorías de manera periódica, incluidas auditorías de los sistemas.

Principio de CONDUCTA HUMANA

Cuestión	Riesgos	Controles
¿Se definen procesos para la incorporación de nuevos recursos y para evitar su salida de la empresa?	• Pérdida de las competencias adquiridas.	• Definir un plan de contratación que se ajuste a las necesidades de la empresa. • Llevar a cabo tareas de formación a los recursos. • Solicitar a los empleados que actualicen su curriculum. • Antes de contratar a nuevas personas o de asignar a un trabajador un nuevo rol, consultar los curriculums de los recursos internos disponibles.
¿Se realizan evaluaciones a los empleados?	• Los trabajadores no están satisfechos. • Metas de negocio inalcanzables.	• Llevar a cabo tareas de formación a los recursos. • Solicitar a los empleados que actualicen su curriculum. • Antes de contratar a nuevas personas o de asignar a un trabajador un nuevo rol, consultar los curriculums de los recursos internos disponibles.
¿Existen empleados, que bien por su conocimiento o por las tareas que realizan, resultan imprescindibles?	• Se puede producir la interrupción y el desajuste de los procesos principales de la entidad. • Pérdidas de beneficios y de capital. • Pérdida de las habilidades y conocimientos adquiridos. • Se daña la imagen corporativa.	• Identificar los roles claves e imprescindibles. • No delegar ciertos conocimientos a una única persona. Hay que garantizar que los recursos comparten habilidades y conocimientos. • Eliminar la dependencia de los roles claves.
¿Existe alguna pauta definida relativa a la sustitución o cambios en los puestos de trabajo?	• Se puede producir la interrupción y el desajuste de los procesos principales de la entidad. • Pérdidas de beneficios y de capital. • Pérdida de las habilidades y conocimientos adquiridos. • Se daña la imagen corporativa.	• Llevar a cabo tareas de formación a los recursos. • Solicitar a los empleados que actualicen su curriculum. • Antes de contratar a nuevas personas o de asignar a un trabajador un nuevo rol, consultar los curriculums de los recursos internos disponibles. • Comunicar al departamento de Recursos Humanos el cambio, si el empleado cambia de proyecto, que queda desasignado, etc.

¿Existe un compromiso en el desarrollo de proyectos T.I de todos los miembros involucrados?	• Metas de negocio inalcanzables. • Se cumplen solo parte de los requisitos de usuario.	• Definir la responsabilidad de todos los miembros de la estructura organizativa y de las partes interesadas. • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas. • Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Se debe elegir una metodología acorde con el tipo de proyectos que se llevan a cabo. • Todos los departamentos de la entidad deben seguir la metodología elegida para optimizar su nivel de madurez.
¿Tras la finalización de un proyecto T.I se realiza transferencia de conocimiento?	• Se puede producir la interrupción y el desajuste de los procesos principales de la entidad. • Pérdida de las habilidades y conocimientos adquiridos.	• Implantar una metodología de proyectos, pues siempre incluyen una tarea de transferencia del conocimiento.
¿Se involucra al personal en todas las etapas de desarrollo de los proyectos T.I, procesos T.I, etc.?	• Los empleados están desmotivados. • Metas de negocio inalcanzables.	• Definir la responsabilidad de todos los miembros de la estructura organizativa y de las partes interesadas. • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas y cómo puede afectar a la consecución de los objetivos de negocio. • Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas. • Se debe elegir una metodología acorde con el tipo de

		proyectos que se llevan a cabo. • Todos los departamentos de la entidad deben seguir la metodología elegida para optimizar su nivel de madurez.
Antes de realizar un cambio en las T.I, ¿se mide la aceptación y el impacto del mismo en las distintas partes involucradas?	• Se rechazan los cambios aunque su implementación pueda generar valor.	• Diseñar e implementar una estructura organizativa y definir las funciones y responsabilidades de cada miembro. • Definir una cultura empresarial que manifieste la importancia de llevar a cabo de manera eficaz las tareas asignadas. • Comunicar a todos los departamentos la importancia de definir correctamente sus requerimientos y de su participación para la consecución de los objetivos de negocio.
La elección de un proveedor conlleva siempre unos riegos asociados, que pueden afectar al servicio T.I, ¿están identificados estos riesgos?	• Se puede producir la interrupción y el desajuste de los procesos principales de la entidad. • Pérdidas de beneficios y de capital. • Pérdida de las habilidades y conocimientos adquiridos. • Se daña la imagen corporativa.	• Evaluar en detalle los servicios ofrecidos por los proveedores y elegir aquellos que mejor se adecuen a las necesidades de la empresa, y con menor probabilidad de riesgo. • Elaborar de forma periódica informes de riesgos en que se incluya también el valor asociado al riesgo.
¿El número de recursos humanos es suficiente y poseen los conocimientos adecuados para llevar a cabo las tareas?	• No se tienen los recursos humanos suficientes y necesarios. • La asignación del personal no es correcta. • Los recursos humanos no tienen los conocimientos necesarios. • Hay que externalizar ciertos procesos o servicios. • Pérdida de las competencias adquiridas.	• Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias. • Llevar a cabo tareas de formación a los recursos. • Antes de contratar a nuevas personas o de asignar a un trabajador un nuevo rol, consultar los curriculums de los recursos internos disponibles.

¿Las estimaciones relacionadas con el número de recursos necesarios son correctas?	• Metas de negocio inalcanzables si no se cuentan con el personal suficiente para llevarlas a cabo.	• Asignar los recursos en base a las necesidades del proyecto. • Revisar los recursos existentes con el fin de evitar recursos duplicados, identificar recursos no útiles o carencias.

Anexo V – Prototipo del modelo de autoevaluación

Se incluyen en este anexo los diagramas relacionados con el prototipo y el diseño del modelo de autoevaluación propuesto, que van a permitir: reflejar la funcionalidad; a nivel de base de datos representar el diseño de las tablas, campos definidos y las relaciones correspondientes; y por último el diagrama de navegación.

Casos de Uso

Se representa mediante los casos de uso la funcionalidad que el prototipo debe recoger:

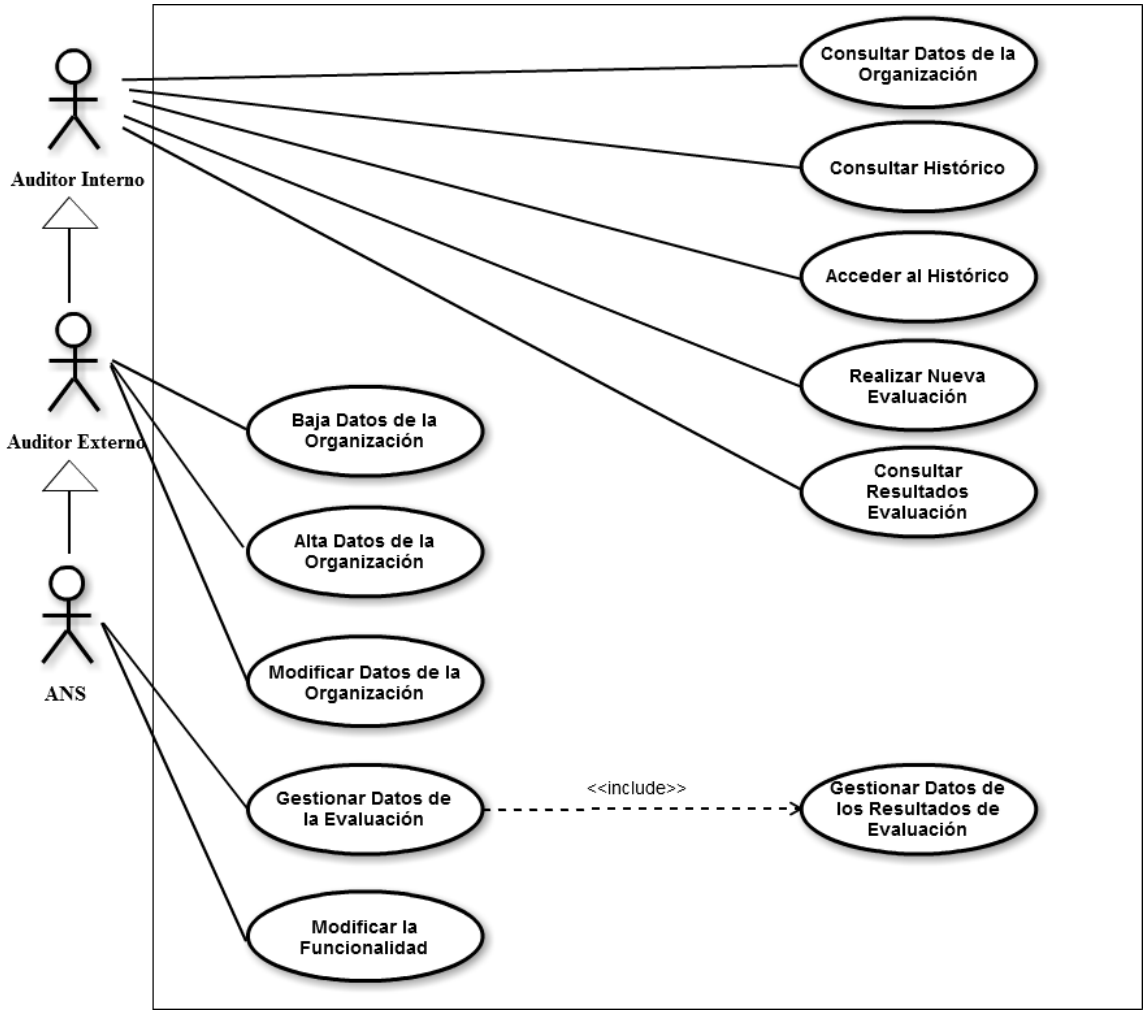

Diagrama relacional

Nos permite representar las entidades definidas, sus atributos, claves y la relación con otras tablas, necesarias para dar soporte al modelo de autoevaluación.

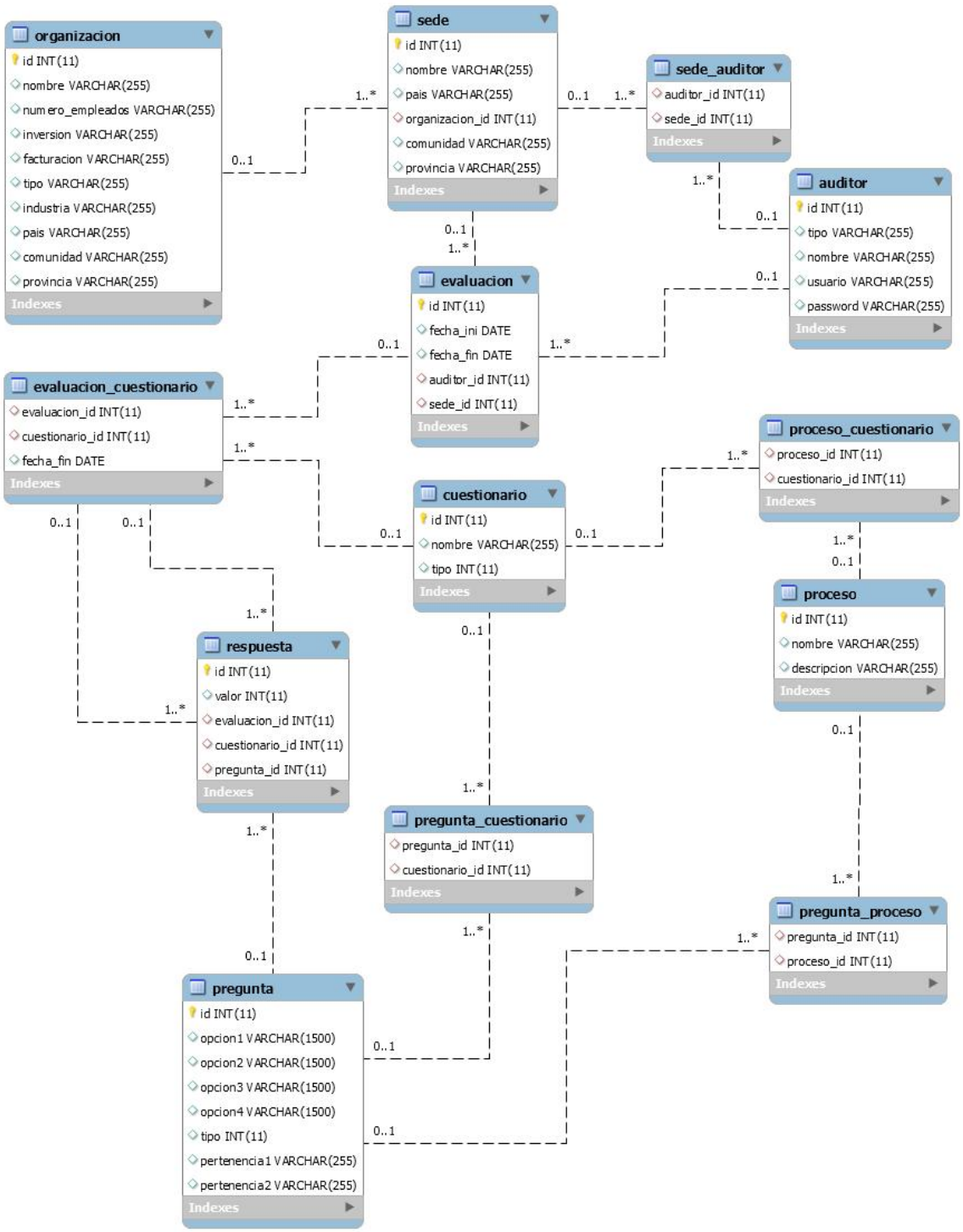

Diagrama de navegación